

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2002 年 2 月 14 日 (14.02.2002)

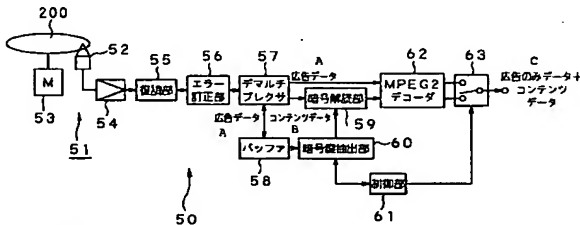
PCT

(10) 国際公開番号
WO 02/13451 A1

- (51) 国際特許分類: H04L 9/00, G06F 17/60, H04N 5/92, G11B 20/10, 20/12
- (21) 国際出願番号: PCT/JP01/06663
- (22) 国際出願日: 2001 年 8 月 2 日 (02.08.2001)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2000-237662 2000 年 8 月 4 日 (04.08.2000) JP
特願2001-133600 2001 年 4 月 27 日 (27.04.2001) JP
- (72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 佐古曜一郎 (SAKO, Yoichiro) [JP/JP]. 工藤淳一 (KUDO, Junichi) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).
- (74) 代理人: 小池 晃, 外(KOIKE, Akira et al.); 〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル Tokyo (JP).
- (81) 指定国 (国内): CA, US.
- 添付公開書類:
— 国際調査報告書
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).
- 2 文字コード及び他の略語については、定期発行される各 PCT ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: CLASSIFIED DATA-CONTAINING DATA RECORDING MEDIUM AND METHOD OF RECORDING/REPRODUCING THE DATA

(54) 発明の名称: 秘匿データを含むデータの記録媒体及びそのデータの記録再生方法



55...DEMODULATION UNIT
56...ERROR CORRECTION UNIT
57...DEMULPLEXER
58...BUFFER
A...ADVERTISEMENT DATA
59...DECODING UNIT
B...CONTENT DATA
60...CIPHER KEY EXTRACTING UNIT
61...CONTROL UNIT
62...MPEG2 DECODER
C...ADVERTISEMENT DATA PLUS CONTENT DATA

(57) Abstract: A recording medium on which content data such as movie data is recorded, wherein a second data such as advertisement data embedded with content data-concealing data is recorded at a position that allows reproduction prior to a first data when the first data consisting of content data is to be reproduced. The first data recorded on this recording medium extracts content concealing data from the second data, decodes the encrypted first data read from the recording medium by using the extracted content concealing data, and is reproduced subsequent to the second data.

(57) 要約:

本発明は、映画等のコンテンツデータが記録された記録媒体であり、コンテンツデータからなる第1のデータを再生する際に第1のデータに先だって再生される位置に、コンテンツデータを秘匿するためのコンテンツ秘匿用データが埋め込まれた広告データの如き第2のデータが記録されている。この記録媒体に記録された第1のデータは、第2のデータからコンテンツ秘匿データを抽出し、抽出されたコンテンツ秘匿データを用いて記録媒体から読み出された第1のデータに施されている暗号を解読し、第2のデータに引き続いて再生される。

WO 02/13451 A1

THIS PAGE BLANK (USPTO)

明細書

秘匿データを含むデータの記録媒体及びそのデータの記録再生方法

技術分野

本発明は、所定データに含ませたコンテンツ秘匿用データに基づいてコンテンツデータを秘匿し、所定データを再生することによってコンテンツ秘匿用データを抽出し秘匿化されているコンテンツデータの再生を可能とした記録媒体及びこの記録媒体の記録又は再生方法に関する。

背景技術

スポンサとして協力のあった会社の広告等の情報を添付して映画、ビデオ映画又はテレビ番組等のコンテンツデータは、テレビジョン放送、ビデオテープカセット、DVD (digital versatile disc) 等の記録媒体を用いて頒布されている。例えば、広告付きでコンテンツが記録された記録媒体は、広告をコンテンツと共に記録することで、低価格で視聴者に提供されている。

近年、音声データ、画像データをはじめとするコンテンツデータは、所謂インターネットの普及によって、ネットワークを介して配信されるようになっている。これに伴って、インターネットのホームページ上には、バナー広告が設けられている。このバナー広告は、ホームページの一部に宣伝のために設けられる広告である。例えば、バナー広告は、利用者がマウス等によりクリック（選択）することによって、宣伝用のウェブページが新たに開かれるようになっている。このとき、バナー広告のクリックされる回数、すなわち利用者のアクセス回数は広告の効果を示す指標ともなっている。

ところで、ビデオテープレコーダ、ハードディスクレコーダ、光ディスクレコーダ等の記録装置の普及に伴い、視聴者は、記録媒体に記録された映画等のコンテンツを好みに合わせて試聴できる。具体的には、視聴者は、読み飛ばし、CM

キャンセラ等の記録装置の種々の機能を利用して、コンテンツのみを視聴できるようにもなった。例えば、上述したように記録媒体には、テレビジョン放送により放送された映画を広告を含めて記録することができるが、視聴者は、映画の本編を鑑賞する際、本編に関係のない広告を再生せずに本編のみを再生することもできる。これでは、広告等のもたらす効果を活かすことができない。このようなことは映画や音楽等のコンテンツに添付される著作権情報としての著作権管理データについても同様にいえることであり、視聴者は、本編に関係のない著作権情報を再生せずに本編のみを再生することができる。

インターネットのバナー広告は、ユーザに対して選択操作（クリック）を強制することができないため、バナー広告の効果は、ユーザの趣向に依存するものとなっていた。

コンテンツを配信する方法としては、暗号化されたコンテンツをインターネット等を介して各端末装置に配信し、別途、このコンテンツの視聴希望者に課金すると共に暗号鍵を提供する方法がある。暗号鍵を視聴希望者に提供するときには、暗号鍵のみをインターネット等を介して提供するのみであって、この暗号鍵には、何ら付加価値が付加されていない。

発明の開示

本発明は、上述したような実情に鑑み提案されるものであって、本発明の目的とするところは、コンテンツデータを再生するために必ず再生が必要な所定データに付加価値を加えることで、コンテンツに添付される広告等の効果を高めることができるデータを記録した記録媒体及び記録方法、更には再生方法を提供することにある。

更にまた、本発明の他の目的は、本発明に係る記録媒体に記録されたデータの送信方法を提供することにある。

上述のような目的を達成するために提案される本発明に係る記録媒体は、コンテンツデータからなる第1のデータを再生する際に第1のデータに先だって再生される位置に、コンテンツデータを秘匿するためのコンテンツ秘匿用データが埋

めこまれた第2のデータが記録されたものである。ここで、第2のデータは、少なくともひとつの広告データであり、この第2のデータは、例えば、複数の広告データからなり、コンテンツ秘匿データは、複数の広告データに分散されて埋め込まれている。

本発明に係る記録媒体に記録方法は、供給された第2のデータにコンテンツデータからなる第1のデータを秘匿するためのコンテンツ秘匿用データを埋め込み、第1のデータをコンテンツ秘匿用データを用いて秘匿処理を施し、コンテンツ秘匿用データが埋め込まれた第2のデータと秘匿処理が施されたコンテンツデータとにエンコード処理を施して記録媒体に記録する。

本発明に係るデータ記録方法は、供給された複数の第2のデータに、コンテンツのデータからなる第1のデータに暗号化処理を施すための暗号鍵データを各々埋めこみ、第2のデータに埋めこまれた暗号鍵データに基づいて第1のデータの少なくとも一部の領域に秘匿処理を施し、コンテンツ秘匿用データが埋めこまれた第2のデータと秘匿処理が施されたコンテンツデータとにエンコード処理を施して記録する。

本発明に係る記録方法によってコンテンツデータが記録された記録媒体を再生する方法は、コンテンツデータからなる第1のデータを再生する際に第1のデータに先だって再生される位置に、コンテンツデータを秘匿するためのコンテンツ秘匿用データが埋めこまれた第2のデータが記録された記録媒体から読み出された第2のデータからコンテンツ秘匿データを抽出し、この抽出されたコンテンツ秘匿データを用いて記録媒体から読み出された第1のデータに施されている暗号を解読し、第2のデータに引き続いて解読された第1のデータを出力する。

また、本発明に係る記録媒体の再生方法は、第1のデータと第2のデータとが記録されるとともに、第2のデータは第1のデータを再生する際に第1のデータよりも先だって読み出される位置に記録され、第1のデータは第2のデータから抜き出されたデータを用いて暗号化処理が施されて記録された記録媒体から第2のデータが読み出され、読み出された第2のデータの所定の領域のデータを抜き出し、抜き出されたデータを用いて記録媒体から読み出された第1のデータに施されている暗号を解読し、第2のデータに引き続いて上記解読された上記第1の

データを出力する。

更に、本発明は、データの送信方法であり、供給された第2のデータにコンテンツデータからなる第1のデータを秘匿するためのコンテンツ秘匿用データを埋め込み、第1のデータを上記コンテンツ秘匿用データを用いて秘匿処理を施し、コンテンツ秘匿用データが埋め込まれた第2のデータと上記秘匿処理が施されたコンテンツデータとにエンコード処理を施して送信する。

また、本発明に係るデータの送信方法は、供給された第2のデータから抜き出したデータを用いてコンテンツデータからなる第1のデータに暗号化処理を施し、第2のデータと暗号化処理が施された第1のデータとにエンコード処理を施して送信する。

本発明に係る再生方法は、コンテンツデータからなる第1のデータを再生する際に第1のデータに先だって再生され、コンテンツデータを秘匿するためのコンテンツ秘匿用データが埋め込まれた第2のデータを含むデータの第2のデータからコンテンツ秘匿データを抽出し、抽出されたコンテンツ秘匿データを用いて第1のデータに施されている暗号を解読し、第2のデータに引き続いて解読された第1のデータを出力する。

本発明に係る他の再生方法は、第1のデータと第2のデータとを含み、第2のデータは第1のデータを再生する際に第1のデータよりも先だって読み出される位置に配され、第1のデータは上記第2のデータから抜き出されたデータを用いて暗号化処理が施されているデータの第2のデータの所定の領域のデータを抜き出し、抜き出されたデータを用いて第1のデータに施されている暗号を解読し、第2のデータに引き続いて解読された第1のデータを出力する。

本発明に係る更に他の再生方法は、コンテンツデータからなる第1のデータがコンテンツ秘匿用データに基づいて暗号化処理が施されて記録された記録媒体の第1のデータを再生装置によって再生する際に、コンテンツ秘匿用データが埋め込まれた第2のデータをネットワークを介して再生装置に取りこみ、取りこまれた第2のデータからコンテンツ秘匿データを抽出し、抽出されたコンテンツ秘匿データを用いて記録媒体から読み出された第1のデータに施されている暗号を解読し、第2のデータに引き続いて解読された第1のデータを出力する。

本発明の更に他の目的、本発明によって得られる具体的な利点は、以下に説明される実施例の説明から一層明らかにされるであろう。

図面の簡単な説明

図 1 は、本発明に用いられる記録装置を示すブロック図である。

図 2 は、記録装置における処理手順の概略を示すフローチャートである。

図 3 は、本発明に用いられる記録装置の他の例を示すブロック図である。

図 4 は、本発明に用いられる再生装置を示すブロック図である。

図 5 は、再生装置における処理手順の概略を示すフローチャートである。

図 6 は、本発明に用いられる再生装置の他の例を示すブロック図である。

図 7 は、画面の所定のラインデータが暗号鍵とされる場合の説明に使用した図である。

図 8 は、所定フレームの画面全体が暗号鍵とされる場合の説明に供する図である。

図 9 は、所定フレームの信号中の帰線消去期間中、すなわち表示画像の外側に位置する部分が暗号鍵とされる場合の説明に供する図である。

図 10 は、各フレームの一部であって、全フレームに亘って暗号鍵が埋め込まれる場合の説明に供する図である。

図 11 は、ウォーターマークにより暗号鍵を埋め込む場合の説明に供する図である。

図 12 は、画像信号のピーク位置に暗号鍵のデータを埋め込む場合の説明に供する図である。

図 13 は、複数の広告データとそれに対応される複数のコンテンツデータとから構成されるデータ形態を示す図である。

図 14 は、複数の広告データの暗号鍵に基づいてコンテンツデータが暗号化される場合の説明に供する図である。

図 15 は、複数の広告データの暗号鍵から 1 つの暗号鍵を生成して、その 1 つの暗号鍵に基づいてコンテンツデータが暗号化される場合の説明に供する図であ

る。

図 1 6 は、広告データが暗号鍵に基づいて暗号化される共に、コンテンツデータが暗号化されている場合の説明に供する図である。

図 1 7 は、複数の広告データの各暗号鍵に対応されてコンテンツデータが部分的に暗号化されている場合の説明に供する図である。

図 1 8 は、一般的なインターネットによって構築されるネットワークシステムを示す図である。

図 1 9 は、本発明が適用されて可能とされたホームページの表示画面を示す図である。

図 2 0 は、ホームページの表示手順を示すフローチャートである。

図 2 1 は、ホームページの表示から暗号化部が解読表示されるまでの処理手順を示すフローチャートである。

図 2 2 は、変速再生やスキップ再生が検出されたとき、暗号鍵に基づいた暗号解読を実行できないようにする再生装置の構成を示すブロック図である。

図 2 3 は、広告付コンテンツの制作についての具体例の説明に使用した図である。

図 2 4 は、本発明が適用された記録装置を説明するブロック図である。

図 2 5 は、本発明が適用された再生装置を説明するブロック図である。

図 2 6 は、サーバ装置に開設されたホームページを説明する図である。

図 2 7 は、再生装置の動作を説明するフローチャートである。

発明を実施するための最良の形態

以下、本発明の実施の形態を図面を参照して詳細に説明する。

(1) 本発明が適用される記録装置

本発明が適用される記録装置 1 0 は、図 1 に示すように、所定データである広告データにコンテンツデータの暗号鍵を埋め込む暗号鍵埋め込み部 1 1 と、M P E G 2 (Moving Picture Experts Group 2) に準拠してビデオデータ等をエンコードするエンコーダ 1 2 と、広告データに埋め込む暗号鍵でコンテンツデータを

暗号化する暗号化部 13 と、コンテンツデータや広告データを時分割多重するマルチプレクサ 14 と、コンテンツデータや広告データにエラー訂正符号化処理を施すエラー訂正部 15 と、コンテンツデータや広告データに変調処理を施す変調部 16 と、ディスク 200 にコンテンツデータや広告データを記録するための記録処理を施す信号記録部 18 を備える。信号記録部 18 は、例えば、光学ヘッド 19、スピンドルモータ 20 等を備える。

このような記録装置 10 には、コンテンツデータ、例えば映像データと、このコンテンツデータを秘匿、例えば暗号化するためのコンテンツ秘匿用データとなる暗号鍵を含む所定データ、例えば広告データとが入力される。暗号化部 13 は、広告データの一部である暗号鍵に基づいてコンテンツデータを秘匿、例えば暗号化する秘匿手段となる。また、マルチプレクサ 14、エラー訂正部 15、変調部 16、アンプ 17 及び信号記録部 18 は、暗号鍵を含む広告データと暗号化されたコンテンツデータとを記録媒体である例えばディスク 200 に記録する記録手段となる。暗号鍵は、再生装置で広告データが再生されることによって抽出されるものであり、この暗号鍵によって、コンテンツデータは、暗号解読が可能となる。

この記録装置 10 は、図 2 に示すような処理を実行する。記録装置 10 は、ステップ S1 において、暗号鍵に基づいてコンテンツデータを暗号化して、続くステップ S2 において、暗号鍵を広告データに埋め込み、続くステップ S3 において、暗号鍵を含む広告データと暗号化されたコンテンツデータとをディスク 200 に記録する。以下、記録装置 10 について詳細を説明する。

コンテンツデータは、MPEG2 に準拠した方式で符号化するために、MPEG2 エンコーダ 12 に入力される。また、暗号化部 13 には、所定データである広告データが入力される。そして、映画等の映像データのコンテンツデータを暗号化するための暗号鍵（コンテンツ秘匿用データ）は、広告データに暗号鍵を埋め込むため暗号鍵埋め込み部 11 に入力されると共に、コンテンツデータを暗号化するため暗号化部 13 に入力される。

暗号鍵埋め込み部 11 は、暗号鍵を広告データの中に埋め込む処理を行う。広告データに暗号鍵を埋め込む処理については後で詳述する。暗号埋め込み部 11

によって暗号鍵が埋め込まれた広告データは、MPEG2エンコーダ12に入力される。

MPEG2エンコーダ12は、MPEG2 (Moving Picture Experts Group 2) の規格に準拠して構成された符号化器であり、コンテンツデータと暗号鍵が埋め込まれた広告データを時間軸及び空間軸方向に圧縮し、エンコード処理する。MPEG2エンコーダ12は、エンコード処理したコンテンツデータを暗号化部13に出力すると共に、エンコード処理した広告データをマルチプレクサ14に出力する。

暗号化部13は、入力された暗号鍵に基づいてエンコード処理されたコンテンツデータを暗号化する。暗号化部13は、暗号化されたコンテンツデータを、マルチプレクサ14に出力する。

マルチプレクサ14は、コンテンツデータと暗号鍵が埋め込まれている広告データとを例えば時分割多重する。時分割多重された信号は、エラー訂正部15に入力される。時分割多重された信号は、エラー訂正部15においてエラー訂正されて、変調部16において変調処理されて、アンプ17によって増幅される。光学ヘッド19は、アンプ17からの信号をスピンドルモータ20によって回転駆動されるディスク200にデータを記録する。

ここで、ディスク200に書き込まれた信号は、暗号鍵が埋め込まれた広告データと該暗号鍵によって暗号化されたコンテンツデータ（映画データ等）からなる。この記録装置10は、再生装置で暗号化されたコンテンツデータを再生するに先立ち、広告データを再生するようにデータを記録する。例えば、内周側からデータを再生するディスクでは、内周側に広告データを記録し、その外周側にコンテンツデータを記録するようにし、また、外周側からデータを再生するディスクでは、外周側に広告データを記録し、内周側に、コンテンツデータを記録するようにする。

以上のような記録装置10は、上述したように、暗号鍵（所定データ）に基づいてコンテンツデータを秘匿、例えば暗号化（解読不能な状態に変換）して、また該暗号鍵を広告データに埋め込み、コンテンツデータと広告データとを広告データの再生に先立って広告データが再生されるようにディスク200に記録する

ことができる。

記録装置 10 は、暗号鍵埋め込み部 11 の後段に M P E G 2 エンコーダ 12 を配置した構成を有しているが、M P E G 2 エンコーダ 12 を暗号鍵埋め込み部 11 の前段に配置するようにしてもよい。この場合、符号化された広告データに対して暗号鍵の埋め込みがなされる。また、M P E G 2 エンコーダ 12 は、暗号化部 13 の後段に配置してもよい。

この記録装置 10 では、コンテンツデータの秘匿を、暗号鍵を用いて行ったが、本発明はこれに限定されるものではなく、例えば、コンテンツデータに対して何らかのデータ変換処理を施すようにしてもよい。この場合、コンテンツデータの秘匿のためのデータ変換は、所定の鍵データ等の秘匿用データに基づいてコンテンツデータに対してなされるスクランブル（例えば、ラインシャッフリングやモザイク等）、外乱付加（例えば、特定ラインへのノイズ外乱付加等）等の処理である。すなわち、ここでいうコンテンツデータの秘匿とは、ある特定のユーザ以外、すなわち、正しい暗号鍵を所有するユーザ以外は、コンテンツデータを正常に再生できなくなるような状態へ変換することであり、コンテンツデータを解読不能にするような状態又は視聴者が映像を見ることを妨げ若しくは音楽を聞くことを妨げる状態にすることである。

記録装置 10 において、マルチプレクサ 14 は、コンテンツデータと広告データとを時分割多重しているが、これに限定されるものではない。例えば、コンテンツデータと広告データとを空間分割してもよい。この場合、後述する再生装置のデマルチプレクサでは、これに対応してコンテンツデータと広告データとを分割するようにする。

以上の例では、暗号鍵を含むデータとされる所定データとして広告データを例に挙げて説明したが、これに限定されるものではない。例えば、対応されるコンテンツデータが映画等著作権管理が必要なデータであるときには、上述の所定データを著作権管理情報とすることもできる。ここで、著作権管理情報とは、コンテンツデータの著作権者のデータ、管理番号等である。

次に、記録装置の他の例を説明する。上述した記録装置 10 は、例えば広告データに全く関係のない暗号鍵に基づいてコンテンツデータを暗号化するものであ

るが、以下に説明する記録装置は、広告データの一部を使用して、コンテンツデータを秘匿、例えば暗号化するものである。ここで、広告データの一部とは、詳細は後述するが例えば所定のフレーム全体又は所定フレーム内のラインデータ等である。

この記録装置 30 は、図 3 に示すように、広告データから所定領域を抽出する所定領域抜き出し部 31 と、コンテンツデータを暗号化する暗号化部 32 と、コンテンツデータや広告データを時分割多重するマルチプレクサ 33 と、コンテンツデータや広告データに対してエラー訂正符号化処理を施すエラー訂正部 34 と、コンテンツデータや広告データに対して変調処理を施す変調部 35 と、ディスク 200 に記録するコンテンツデータや広告データを増幅するアンプ 36 と、コンテンツデータや広告データをディスク 200 に記録するための記録処理を施す信号記録部 37 を備える。この記録装置 30 は、図 1 に示した記録装置 10 と同様な動作となり、基本的な動作としては図 2 に示すものと同様であるが、ステップ S2 において暗号鍵を広告データに埋め込む処理はなく、その代わりに、ステップ S1 において、広告データの所定領域から暗号化に使用するデータを抜き出して、その抜き出したデータに基づいてコンテンツデータを暗号化する。以下、記録装置 30 について詳細を説明する。

この記録装置 30 は、所定領域データ抜き出し部 31 を備えることを特徴とする。この記録装置 30 は、この所定領域データ抜き出し部 31 によって広告データの所定領域からデータを抜き出して（抽出して）、その抜き出したデータ（以下、暗号化用データという。）を暗号化部 32 に入力するようにしている。

暗号化部 32 には、コンテンツデータが入力され、暗号化部 32 は、このコンテンツデータを、所定領域データ抜き出し部 31 で抜き出された暗号化用データに基づいて暗号化する。この暗号化部 32 で暗号化されたコンテンツデータは、マルチプレクサ 33 に入力される。

マルチプレクサ 33 には、暗号化されたコンテンツデータと共に広告データが入力され、この広告データとコンテンツデータとを時分割多重する。このマルチプレクサ 33 において時分割多重されたデータは、以後、上述の記録装置 10 と同様な処理手順に沿って処理がされる。すなわち、時分割多重されたデータは、

エラー訂正部 34 においてエラー訂正されて、変調部 35 において変調処理されて、アンプ 36 によって増幅される。光学ヘッド 38 は、アンプ 36 からのデータを、スピンドルモータ 39 によって回転駆動されるディスク 200 に書き込む。

この記録装置 30 は、上述したように、広告データの一部を抜き出して、その抜き出したデータ、例えば、暗号化用データに基づいてコンテンツデータを秘匿、例えば暗号化、すなわち解読不能な状態に変換して、コンテンツデータと広告データとがコンテンツデータの再生に先立って広告データが再生されるようにディ

記録装置 30 は、上述したように記録装置 10 が限定的に解釈されないことと同様に、上述の説明に限定されるものではない。

(2) 本発明が適用される再生装置

本発明が適用される再生装置 50 は、上述の図 1 に示した記録装置 10 によってデータが記録されたディスク 200 を再生するための装置であり、図 4 に示すように、ディスク 200 よりデータを読み出す信号再生部 51 と、信号再生部 51 で読み出したデータを増幅し RF 信号等を生成するアンプ 54 と、アンプ 54 より入力されたデータを復調する復調部 55 と、復調されたデータに対してエラー訂正処理を施すエラー訂正部 56 と、時分割多重された信号を広告データとコンテンツデータとに分割するデマルチプレクサ 57 と、広告データを一時的に蓄積するバッファ 58 と、コンテンツデータの暗号を解読する暗号解読部 59 と、広告データより暗号鍵を抽出する暗号鍵抽出部 60 と、MPEG2 でエンコードされたデータをデコードする MPEG2 デコーダ 62 と、データの出力を切り換えるデータ出力切換部（スイッチ）63 と、データ出力切換部 63 を制御する制御部 61 とを備える。ここで、信号再生部 51 は、例えば、光学ヘッド 52 及びスピンドルモータ 53 を備える。

このような再生装置 50 は、コンテンツデータを秘匿、例えば暗号化するための暗号鍵を含む広告データと暗号化されたコンテンツデータとが記録された記録媒体であるディスク 200 から暗号化されたコンテンツデータを読み出して再生するものであり、暗号鍵抽出部 60 は、コンテンツデータの再生に先行して、広告データを再生して暗号鍵を抽出する抽出手段となる。暗号解読部 59 は、広告データより抽出された暗号鍵に基づいて暗号化されたコンテンツデータの暗号を

解読する秘匿解除手段となる。更に、暗号解読部 59 以降の M P E G 2 デコーダ 62 等は、暗号化が解除されたコンテンツデータを再生する再生手段となる。

この再生装置 50 は、図 5 に示すような処理を実行する。すなわち、図 5 に示すように、再生装置 50 は、ステップ S 11 において、コンテンツデータに先行して、広告データを再生して暗号鍵を抽出し、続くステップ S 12 において、抽出された暗号鍵に基づいて暗号化されたコンテンツデータを暗号解読し、続くステップ S 13 において、暗号解読されたコンテンツデータを再生する。以下、再生装置 50 について詳細を説明する。

再生装置 50 は、スピンドルモータ 53 によって、例えば線速度一定又は角速度一定で回転駆動されているディスク 200 から光学ヘッド 52 によって信号を読み取る。ここで、読み取られた信号は、例えば時分割多重された信号であって、暗号鍵が埋め込まれた広告データと暗号鍵によって暗号化された映画等のコンテンツデータである。

光学ヘッド 52 から出力された信号は、アンプ 54 において増幅処理されて、復調部 55 で復調処理されて、更にエラー訂正部 56 においてエラー訂正処理がなされる。エラー訂正部 56 においてエラー訂正された信号（時分割多重された信号）は、デマルチプレクサ 57 に入力される。

デマルチプレクサ 57 は、入力された時分割多重された信号を広告データとコンテンツデータとに分割する。デマルチプレクサ 57 にて分割して得られた広告データは、バッファ 58 及び M P E G 2 デコーダ 62 に入力される。デマルチプレクサ 57 にて分割して得られたコンテンツデータは、暗号解読部 59 に入力される。ここで、暗号解読部 59 に入力されるコンテンツデータは、暗号鍵に基づいて暗号化されている。

暗号鍵抽出部 60 は、バッファ 58 に取り込まれた広告データから暗号鍵を抽出して、抽出した暗号鍵を暗号解読部 59 に出力する。

暗号解読部 59 には、暗号化されているコンテンツデータを、暗号鍵抽出部 60 にて抽出された暗号鍵に基づいて解読（復号）する。暗号解読部 59 にて解読されたコンテンツデータは、M P E G 2 デコーダ 62 に入力される。

M P E G 2 デコーダ 62 は、M P E G 2 (Moving Picture Experts Group 2)

の規格に準拠して構成された復号器であり、コンテンツデータは、ここでMPEG 2方式によってデコード処理される。また、MPEG 2デコーダ62には、デマルチプレクサ57にて分割して得られた広告データが入力され、ここで、広告データはデコード処理される。デコード処理されたコンテンツデータ及び広告データは、データ出力切換部63に入力される。

データ出力切換部63は、制御部61により制御されて、所定のタイミングで、MPEG 2デコーダ62からの広告データをモニタ、スピーカ等の後段のブロックに出力する。また、データ出力切換部63は、制御部61により制御されて、所定のタイミングで、MPEG 2デコーダ62からのコンテンツデータをモニタ、スピーカ等の後段のブロックに出力する。このような制御部61による制御により、コンテンツデータに先行して、対応する広告データが出力される。

再生装置50は、広告データをディスク200から読み出すことができないとき、暗号鍵を抽出することができないためにコンテンツデータを暗号解読することができない。また、再生装置50は、暗号鍵抽出部60にて広告データから暗号鍵を抽出することができないときにもコンテンツデータを暗号解読することができない。したがって、このような場合には、再生装置50では、コンテンツデータを再生することができなくなる。

以上、再生装置50は、上述したように、広告データに埋め込まれている暗号鍵を抽出して、その暗号鍵に基づいてコンテンツデータを暗号解読することにより、コンテンツデータと広告データと再生することができる。再生装置50は、このような再生を暗号鍵が抽出された広告データを先行して行うようにしている。これにより、再生装置50は、映画等のコンテンツデータを見たい視聴者に、強制的に広告データを先行して見せるようにすることができる。これにより、再生装置50は、コンテンツに添付される広告効果を高めることができる。

再生装置50は、暗号解読部59の後段にMPEG 2デコーダ62が配置されたものであるが、MPEG 2デコーダ62を暗号解読部59の前段に配置するようにしてもよい。具体的には、MPEG 2デコーダ62を配置する位置は、上述の記録装置10におけるMPEG 2エンコーダ12の配置される位置に対応して決定する。

上述の再生装置 50 では、コンテンツデータの秘匿が暗号鍵を用いて行っただが、本発明はこれに限定されるものではなく、例えば、コンテンツデータの秘匿は、コンテンツデータに対しての何らかのデータ変換処理を施すことにより行うようにしてもよい。この場合、コンテンツデータの秘匿の解除は、コンテンツデータに対してなされているスクランブル（例えば、ラインシャッフリングやモザイク等）、外乱付加（例えば、特定ラインへのノイズ外乱付加等）又はブルーバック等の解除となる。上述したように、ここでいうコンテンツデータの秘匿とは、ある特定のユーザ、すなわち正しく暗号鍵を入手できるユーザ以外にはコンテンツデータを正常に再生できなくなるような状態へ変換することであり、コンテンツデータを解読不能にするような状態又は視聴者が映像を見ることを妨げ若しくは音楽を聞くことを妨げる状態にするである。秘匿解除は、このような解読不能とされていることの解除又はこのような妨げの解除となる。

デマルチプレクサ 57 は、コンテンツデータと広告データとを時分割多重した信号を分割しているが、これに限定されるものではない。例えば、コンテンツデータと広告データとが空間分割されている信号を分割してもよい。

次に、本発明が適用された再生装置の他の例について説明する。上述の再生装置 50 は、暗号鍵に基づいてコンテンツデータを暗号解読するものであったが、ここで説明する再生装置 70 は、広告データの一部である暗号化用データに基づいてコンテンツデータを暗号解読するように構成されている。

再生装置 70 は、図 6 に示すように、ディスク 200 よりデータを読み出す信号再生部 71 と、信号再生部 51 で読み出したデータを増幅し RF 信号等を生成するアンプ 74 と、アンプ 54 より入力されたデータを復調する復調部 75 と、復調されたデータに対してエラー訂正処理を施すエラー訂正部 76 と、時分割多重された信号を広告データとコンテンツデータとに分割するデマルチプレクサ 77 と、広告データより暗号鍵として用いられている所定領域を抽出する所定領域データ抽出部 78 と、コンテンツデータの暗号を解読する暗号解読部 79 と、データの出力を切り換えるデータ出力切換部（スイッチ）81 と、データ出力切換部（スイッチ）63 を制御する制御部 80 とを備える。この再生装置 70 は、図 4 に示した再生装置 50 と同様な動作となり、基本的な動作は図 5 に示すものと

同様であるが、ステップS 1 1において、広告データを再生して暗号化鍵を抽出するのではなく、暗号化に使用した暗号化用データを広告データの所定領域から抽出して、ステップS 1 2において、その抽出した暗号化用データに基づいて暗号化されたコンテンツデータを暗号解読する。以下、再生装置70について詳細を図6を参照して説明する。

この再生装置70は、デマルチプレクサ77からの広告データが入力される所定領域データ抽出部78を備えているところに特徴がある。再生装置70は、この所定領域データ抽出部78によって広告データの所定領域から暗号化に使用した暗号化用データを抽出して、その暗号化データを暗号解読部79に出力している。

暗号解読部79には、暗号化されているコンテンツデータが入力されており、この暗号化されているコンテンツデータを、所定領域データ抽出部78で抽出された暗号化用データに基づいて暗号解読する。この暗号解読部79にて暗号解読されたコンテンツデータは、データ出力切換部81に入力される。

データ出力切換部81は、上述の再生装置50の場合の動作と基本的には動作が同様であり、制御部80により制御されて、所定のタイミングで、デマルチプレクサ77からの広告データを後段のブロックに出力する。データ出力切換部81は、制御部80により制御されて、所定のタイミングで、暗号解読部79からのコンテンツデータを後段のブロックに出力する。このような制御部80による制御により、コンテンツデータに先行して、対応される広告データの出力がなされるようになる。

再生装置70は、広告データをディスク200から読み出すことができないときや所定領域データ抽出部78にて広告データから暗号化用データを抽出することができないとき、コンテンツデータを暗号解読することができないので、コンテンツデータを再生を中止する。

以上のように、再生装置70は、広告データから暗号化用データを抽出して、この抽出した暗号化用データに基づいてコンテンツデータを暗号解読することにより、コンテンツデータと広告データと再生することができる。再生装置70は、そのような再生を暗号化用データが抽出された広告データを先行して行うように

している。これにより、再生装置 70 は、コンテンツデータ（映画等）を見たい視聴者に、強制的に広告データを先行して見せるようにすることができる。これにより、コンテンツに添付される広告の効果は、有効なものになる。

上述の再生装置 70 は、上述したように再生装置 50 が限定的に解釈されないことと同様に、上述の説明に限定されるものではない。

（３）暗号化に使用される広告データの暗号鍵用データ及び広告データへの暗号鍵の埋め込み等

暗号化に使用される広告データとは独立のデータである暗号鍵の広告データへの埋め込み、又は広告データの一部データを暗号鍵として用いる場合について説明する。

図 1 に示した記録装置 10 の暗号鍵埋め込み部 11 における広告データへの暗号鍵の埋め込みは、図 7 に示すように、広告データの所定フレーム画面 P の所定のラインに暗号鍵 d を埋め込むようにする。一方、図 2 に示した記録装置 30 の所定領域抜き出し部 31 における広告データからの暗号化用データの抜き出しについては、図 7 に示すような広告データの所定フレーム画面 P の所定のラインデータ d をそのまま暗号化用データとして抜き出すようにする。再生装置側では、このような広告データへの暗号鍵の埋め込みや、広告データからの暗号化用データの抜き出しに対応して、暗号鍵を抽出してコンテンツデータを暗号解読し、又は暗号化用データを抽出してコンテンツデータを暗号解読する。

図 2 に示した記録装置 30 の所定領域抜き出し部 31 における広告データからの暗号化用データの抜き出しについては、図 8 に示すような広告データの所定フレーム画面 P 全体のデータを暗号化用データとして抜き出すようにする。再生装置側では、このような広告データからの暗号化用データの抜き出しに対応して、暗号化用データを抽出してコンテンツデータを暗号解読する。

図 1 に示した記録装置 10 の暗号鍵埋め込み部 11 における広告データへの暗号鍵の埋め込みは、図 9 に示すように、広告データの所定フレームの信号中の帰線消去期間中、すなわち表示画面 P の外側に位置する部分に暗号鍵 d を埋め込むようにする。例えば、図 9 に示すように表示画面 P の下側に暗号鍵を埋め込むか、表示画面 P の上側に暗号鍵を埋め込む。再生装置側では、このような広告データ

への暗号鍵の埋め込みに対応して、暗号鍵を抽出してコンテンツデータを暗号解読する。

暗号化鍵は、広告データとしての広告映像を構成する全フレームに亘って埋め込むようにすることもできる。具体的には、図10に示すように、全フレームに亘って該各フレーム画面Fの一部にデータ（暗号鍵の一部）dを埋め込み、全データ（暗号鍵の全部）dの取得、例えば、加算、蓄積（アキュムレート）によって暗号鍵が生成されるようにする。これにより、広告映像全体を再生しない限り、全データdをアキュムレート等できないために暗号鍵の取得をできないようにして、コンテンツデータの暗号解読を不可能にすることができる。なお、広告映像を構成する全フレームに亘って各フレーム画面Fの一部のデータdを暗号化用データとすることもできる。

このような暗号鍵の埋め込みを採用すれば、視聴者は、広告映像全体を再生しない限り、コンテンツデータを見ることができないようになる。例えば、一部のフレームのみに暗号鍵を埋め込んだときには、フレームのみ再生すれば本編の暗号解読がなされ、本編全体を見ることができるようになる。しかし、広告映像を構成する全フレームに亘って暗号鍵を一部ずつを埋め込むことにより、広告映像全体を再生しない限り、暗号鍵が生成されず、本編が暗号解読されないようにすることができる。このように、コンテンツデータを見るためには広告映像全体を再生することを前提とすることにより、広告効果を効果的なものとすることができる。

また、このようなフレーム間に亘って暗号鍵を埋め込むとき、広告映像の所定時間内、例えば、30秒の広告映像に対して20秒間のフレームにのみ埋め込むようにしてもよい。これにより、視聴者は、所定時間だけ広告映像を見ることにより、本編を見ることができるようになる。

暗号鍵は、図11に示すように、画像信号中の下位データに埋め込むことができる。このような画像信号の下位データへのデータの埋め込みとしては、電子透かし（ウォーターマーク）によるデータの埋め込み技術が挙げられる。ウォーターマークとは、例えば所謂SDMI（Secure Digital Music Initiative）において規格化されたコピー管理情報の入る電子透かしである。

暗号鍵のデータは、図 1 2 に示すように、画像信号のピーク位置に埋め込むこともできる。一方、画像信号のピーク値の下位データを抜き出して暗号用データとして使用することもできる。例えば、画像信号のピーク値とは、輝度信号のピーク値である。

暗号鍵は、スペクトラム拡散により、画像信号中に埋め込みこともできる。

以上のように、暗号化に使用される暗号鍵（広告データとは独立のデータ）の広告データへの埋め込み又は広告データの一部データである暗号化用データが決定されるが、上述したような例に限定されないことはいうまでもない。

（４）複数の広告データを使用した例

上述した記録装置 1 0，3 0 や再生装置 5 0，7 0 では、1 つの暗号鍵としての広告データに 1 つのコンテンツデータが対応している場合を例として説明した。例えば、図 1 3 に示すようなデータ形態のように、複数の広告 1、広告 2、広告 3、広告 4、・・・に対して複数のコンテンツデータ A、コンテンツデータ B、コンテンツデータ C、・・・が対応されたような場合である。このようなデータ形態は、シリアル方式に対応された形態となっているが、これに限定されるものではなく、データ形態は、パラレル方式に対応された形態とされていてもよい。

複数の広告データ（複数の暗号鍵又は複数の暗号化用データ）に暗号化対象として 1 つのコンテンツを対応させることもできる。以下の説明では、複数の暗号鍵（広告データとは独立しているデータ）に基づいて行うコンテンツデータ A の暗号化及び暗号解読を説明するが、広告データの一部のデータを暗号化用データとして使用しコンテンツデータ A の暗号化及び暗号解読ができるようにしてもよい。複数の暗号鍵に基づいて行うコンテンツデータ A の暗号化及び暗号解読は具体的には次のようになされる。

例えば、図 1 4 に示すように、広告 1 ～ 広告 4 の 4 個の広告データに埋め込まれる暗号鍵の一又は複数を用いてコンテンツデータ A を暗号化する。例えば、広告 1 ～ 4 に同じ暗号鍵を埋め込み、広告 1 ～ 広告 4 の何れかを再生することにより、暗号鍵を取得するようにする。これにより、再生装置は、広告 1 ～ 広告 4 の何れか 1 つを再生することによって、コンテンツデータ A の暗号を解読し再生することができるようになる。

コンテンツデータ A を暗号化する暗号鍵を広告 1 ～ 広告 4 に分散して埋め込むようにし、広告 1 ～ 広告 4 の全てを再生することにより、暗号鍵を取得することができるようにしてもよい。これにより、再生装置は、広告 1 ～ 広告 4 の全てを再生することによってのみ、暗号鍵を取得し、コンテンツデータ A の暗号を解読し、再生することができるようになる。

例えば、複数の広告データに埋め込まれる暗号鍵を用いて先ず 1 つの暗号鍵を生成して、その生成した 1 つの暗号鍵によってコンテンツデータを暗号化するようにしてもよい。具体的には、図 15 に示すように、広告 1 ～ 広告 4 の 4 個の広告データに埋め込まれる暗号鍵を用いて、一方向性関数である Hash 関数により 1 つの暗号鍵を生成して、その暗号鍵に基づいてコンテンツデータ A を暗号化するようにする。

広告データ自体を他の広告データの暗号鍵に基づいて暗号化するようにしてもよい。例えば、暗号解読の場合について説明すると、図 16 に示すように、広告 1 の広告データに埋め込まれる暗号鍵に基づいて広告 2 の広告データを暗号解読する。これにより、広告 2 の広告データから広告 3 の広告データの暗号解読に使用する暗号鍵を得ることができる。広告 2 の広告データから得た暗号鍵に基づいて広告 3 の広告データを暗号解読して、広告 4 の広告データの暗号解読に使用する暗号鍵を得る。次いで、広告 4 の広告データの暗号解読用の暗号鍵に基づいて広告 4 の広告データの暗号解読して得た暗号鍵（コンテンツデータ A 用の暗号鍵）によってコンテンツデータ A の暗号解読をする。このように、広告データを、所謂チェーン式に暗号解読できるようにすることで、必ず広告 1 から広告 4 の順番で再生していかなければコンテンツデータ A を見ることはできないようにすることができる。このような場合の広告データ及びコンテンツデータ A の暗号化については、この逆の手順によって実現されるものであり、すなわち、コンテンツデータ A 用の暗号化に使用した暗号鍵を広告 4 の広告データに埋め込んで暗号化して、広告 4 の広告データの暗号化に使用した暗号鍵を広告 3 の広告データに埋め込んで暗号化して、広告 3 の広告データの暗号化に使用した暗号鍵を広告 2 の広告データに埋め込んで暗号化して、広告 2 の広告データの暗号化に使用した暗号鍵を広告 1 の広告データに埋め込むようにすればよい。

複数の広告データに埋め込まれる各暗号鍵によって、画像を部分的に暗号化してもよい。具体的には、図17に示すように、広告1～広告4の各広告データに埋め込まれる暗号鍵により、4分割されるコンテンツデータAのそれぞれ対応される領域A(1)～領域(4)を暗号化する。

このようにすることで、全ての広告データを再生しない限り、すなわち、全ての暗号鍵を取得しない限りコンテンツデータAの全画面を表示することができないようにすることができる。すなわち、広告1の広告データが再生されただけでは、コンテンツデータAの一部の領域(1)だけが再生(暗号解読)されるようになる。

(5) インターネットのホームページの表示への適用例

上述の記録装置10、30及び再生装置50、70について、コンテンツデータ及び広告データとして映像を対象として説明したが、本発明は、所謂インターネットのホームページの表示にも適用することができる。例えば、インターネットを利用したネットワークシステムは、図18に示すように、サーバ装置100と複数のパーソナルコンピュータ(PC)等の端末装置1101～110nとがインターネット111を介して接続されている。

ここで、サーバ装置100は、制御部101及びデータ蓄積装置102を備えている。データ蓄積装置102は、大記憶容量ハードディスクドライブ等からなり、ネットワーク(例えば、インターネット111)を介してデータの送受信を行うデータ、例えば端末装置1101～110nからの要求信号に応じて送信するホームページを構成する表示データや音声データ等が蓄積されている。すなわち、データ蓄積装置102には、コンテンツデータの広告であるバナー広告の表示データや、バナー広告が操作(クリック)されたときに、再生される広告データや、コンテンツデータ等が蓄積されている。サーバ装置100は、端末装置1101～110nからのアクセス要求に応じて所定のURLのホームページを構成する表示データ等を端末装置1101～110nに送信する。端末装置1101～110nは、サーバ装置100から送信されたデータを受信すると、CRT(cathode ray tube)、LCD(liquid crystal display)等の表示部に表示データを表示する。

例えば、図19は、サーバ装置100より端末装置1101～110nに送信されたホームページ画面120を示している。サーバ装置100は、制御部101の制御に応じて端末装置1101～110nからのアクセス要求に対して画面120を表示するための表示データ等を送信する。

端末装置1101～110nは、図20に示すように、ステップS21において、コンテンツデータを再生するための広告バナーを有する画面を表示し、続くステップS22において、画面上の広告バナーの操作（クリック）に応じて暗号鍵を含む広告データを再生し、続くステップS23において、広告データの再生に応じて暗号鍵を抽出し、続くステップS24において、抽出された暗号鍵に基づいてコンテンツデータを再生する。以下、詳細を説明する。

このサイトXYZ（ホームページの仮称）の画面120上には、図19に示すように、略中央付近に平文情報部122と、暗号化情報部123とが表示されている。暗号化情報部123は、該ホームページを見ている者にとっては見逃すことのできない情報を提供しているのであるが、通常状態においては秘匿、例えば暗号鍵（暗号化用データ）によって暗号化されている。例えば、暗号化情報部123は、モザイク等がかけられ又は背景画面（青色等）等とされている。平文情報部122は、通常状態において、読むことができるようになされている。

サイトXYZの画面120上には、画面の端側にバナー広告が表示されている。画面120では、バナー広告1（1211）、バナー広告2（1212）、バナー広告3（1213）、バナー広告4（1214）といったように4つのバナー広告が表示されている。

このような画面表示がなされている場合においてバナー広告をクリックすることによって、広告データが表示（再生）されて、広告データの表示（再生）に応じて暗号鍵の抽出がなされる。例えば、広告データの表示は、画面の一部への表示によりなされたり、該サイトXYZの画面上への新たな画面によりなされたりする。このような広告データの表示に応じて抽出された暗号鍵に基づいて暗号化情報部（コンテンツデータ）123にかかっているモザイク等が解除される。具体的には、4つの全てのバナー広告がクリックされない限り、暗号化情報部123にかかっているモザイクが解除されないようになされていたり、又はそれぞれ

のバナー広告のクリックに対応して暗号化情報部 1 2 3 にかかっているモザイクが部分的に解除されていくようになされている。

端末装置 1 1 0 1 ~ 1 1 0 n は、図 2 1 に示すように暗号化情報部 1 2 3 の暗号を解読する、すなわちモザイク等が解除されるまでの具体的な処理手順を示している。ここでは、少なくとも 1 つの広告バナーが選択されたときに暗号化情報部 1 2 3 のモザイク等を解除する例を説明する。

ステップ S 3 1 において、端末装置 1 1 0 1 ~ 1 1 0 n には、ホームページの画面表示がされる。続くステップ S 3 2 において、端末装置 1 1 0 1 ~ 1 1 0 n は、「どれか広告をクリックして下さい」といった広告バナーの選択を促す表示をする。ステップ S 3 3 において、端末装置 1 1 0 1 ~ 1 1 0 n は、広告バナーが選択されたか否かの判別を行う。このステップ S 3 3 において、端末装置 1 1 0 1 ~ 1 1 0 n は、広告 1 ~ 広告 4 のどれかがクリックされるまで、ステップ S 3 2 の処理として「どれか広告をクリックして下さい」といった表示をし続け、広告 1 ~ 広告 4 のどれかがクリックされると、ステップ S 3 4 に進むようになる。

ステップ S 3 4 において、端末装置 1 1 0 1 ~ 1 1 0 n は、クリックされた広告 (n) から暗号鍵を入手 (抽出) して、続くステップ S 3 5 において、入手した暗号鍵に基づいて暗号化情報部 1 2 3 を解読して表示する。なお、広告バナーのクリックに対応して広告データを再生してから、暗号化情報部 1 2 3 を再生 (解読) するようになっているが、広告バナーのクリックのみで暗号化情報部 1 2 3 を直ちに再生するようにしてもよい。

(6) その他の例

再生装置は、広告データの変速再生やスキップ再生の検出部を設けて、検出部において変速再生やスキップ再生が検出されたとき、暗号鍵に基づいた暗号解読を実行できないようにすることもできる。図 2 2 には、そのような処理を実現するために再生装置の備える構成を示している。

再生装置は、図 2 2 に示すように、広告データを通常再生しているかを判別する広告データ再生モニタ部 1 3 1 と、広告データより暗号鍵を抽出する暗号鍵抽出部 1 3 3 と、広告データが通常再生されているときに限って暗号鍵抽出部 1 3 3 に広告データを出力するようにするスイッチ 1 3 2 と、スイッチ 1 3 2 の切り

換えを制御する制御部 134 と、コンテンツデータの暗合を解除する暗号解読部 135 を備える。例えば、図 4 に示した再生装置 50 と比較したとき、広告データ再生モニタ部 131 及びスイッチ 132 が新たな構成となる。なお、制御部 134 は、このような新たな構成に対応されて新たな制御機能を有するものである。なお、以下の例では、暗号鍵に基づいてコンテンツデータが暗号化されている場合を例として説明するが、広告データの一部とされる暗号化用データに基づいてコンテンツデータが暗号化されている場合にも適用できる。

この図 22 に示すような構成を備えた再生装置には、暗号鍵が埋め込まれた広告データ及び該暗号鍵によって暗号化されたコンテンツデータからなるデータが入力されており、広告データは、広告データ再生モニタ部 131 及び暗号解読部 135 に入力される。暗号解読部 135 には、広告データと共に対応するコンテンツデータも入力される。

広告データ再生モニタ部 131 は、入力された広告データの再生をモニタする。この広告データ再生モニタ部 131 は、広告データが変速再生やスキップ再生等の広告効果を発揮することができないような再生（以下、特殊再生という。）がなされているか否かを検出する。その検出結果は、制御部 134 に出力される。再生モニタ部 131 は、例えば再生装置にも受けられた図示しない高速再生ボタンやスキップ再生のためのボタンが操作され、入力された広告データが通常の再生処理時の転送速度よりも速くなり、あるいは連続して広告データが得られなくなった場合には、広告データが特殊再生されたと検出する。

制御部 134 は、各構成部を制御している。この制御部 134 は、広告データ再生モニタ部 131 の検出結果に応じてスイッチ 132 のオン／オフの切換を制御する。ここで、スイッチ 132 は、広告データ再生モニタ部 131 と暗号鍵抽出部 133 との接続をオン／オフする。

制御部 134 は、広告データ再生モニタ部 131 の検出結果から広告データの再生が特殊再生ではなく通常の再生とされているときには、スイッチ 132 をオンにして、広告データ再生モニタ部 131 から暗号鍵抽出部 133 に広告データを出力するようにする。制御部 134 は、広告データが特殊再生されているときには、スイッチ 132 をオフにして、広告データ再生モニタ部 131 から暗号鍵

抽出部 1 3 3 に広告データを出力しないようにする。

暗号鍵抽出部 1 3 3 は、広告データに埋め込まれている暗号鍵を抽出するものであるが、広告データが変速再生やスキップ再生等の特殊再生されているときには、広告データ再生モニタ部 1 3 1 からの広告データの入力がなくなり、暗号鍵の抽出ができなくなる。なお、これは、広告データが特殊再生されているときには暗号鍵を破壊する、といった処理と同じである。これにより、暗号鍵抽出部 1 3 3 により抽出される暗号鍵によってコンテンツデータの暗号解読を行う暗号解読部 1 3 5 は、広告データが特殊再生されているときには、コンテンツデータの暗号解読が不可能になるため、コンテンツデータの暗号解読処理、コンテンツデータの再生処理を中止する。広告データが特殊再生されたことにより、コンテンツデータの暗号解読ができなかったようなときには、例えばモニタ上にその旨、例えば「不正な操作がなされたので終了します」等の警告表示をして、使用者に注意を促すようにすることもできる。

一方、広告データが通常再生されているときには、暗号鍵抽出部 1 3 3 では、広告データから暗号鍵を抽出することができ、更に暗号解読部 1 3 5 では、その暗号鍵に基づいてコンテンツデータの暗号解読ができる。したがって、広告データが通常再生されているときには、コンテンツデータは、暗号解読された状態として、後段の M P E G 2 デコーダ等へ出力されるようになる。

以上のように、再生装置は、広告データが早送り再生等の変速再生やスキップ再生等の特殊再生が行われたとき、広告データから暗号鍵の抽出を不可能として、暗号鍵に基づくコンテンツデータの暗号解読をできないようにすることができる。これにより、再生装置は、本編を見るためには視聴者に対して広告を通常再生により見ることを要求することができ、これにより、広告効果を有効的なものとすることができる。

上述の例では、特殊再生されたとき、暗号鍵の抽出を不可能にして、コンテンツデータの暗号解読をできないようにしているが、特殊再生されたときに、青画面（例えば、ブルーバック）、ホワイトノイズ等のコンテンツデータの視聴が妨げられるようにすることもできる。

コンテンツデータと広告データとが対応されることが本発明の前提とされるが、

このような所謂広告付きコンテンツの作成は、コンテンツ作成会社で作成するようにしてもよい。その場合の手順を図23を用いて説明する。本例は、図23に示すように、コンテンツ製作会社150にて鍵データ（暗号鍵）による暗号化コンテンツが製作され、広告制作会社151にて鍵付広告CMが製作される場合を示している。

コンテンツ制作会社150では、制作したコンテンツを鍵データ（暗号鍵）Kに基づいて暗号化する。また、広告制作会社151では、コンテンツ制作会社150から送られてくる鍵データKに基づいて、広告に鍵データKを添付した（埋め込んだ）鍵付広告CMを作成する。

コンテンツ制作会社150において、広告作成会社151で作成された鍵付広告CMを使用して、編集作業によって、その鍵付広告CMと該鍵付広告CMに埋め込まれている鍵データKにより暗号化されたコンテンツCとを一体として広告付コンテンツを作成する。このようにして作成された広告付コンテンツをユーザが購入する。

以上の例では、本発明を記録装置、再生装置等に適用した場合について説明したが、更に、本発明を、送信装置や受信装置に適用することもできる。

送信装置については、図1及び図3に示したような記録装置10, 30におけるアンプ17, 36以降の構成を、送信手段に変更するようにすればよい。例えば、送信手段の構成としては、搬送波処理部等が挙げられる。このように、アンプ17, 36以降の構成を、送信手段に変更することによって送信装置とすることができ、アンプ17, 36の前段までの処理は、上述した記録装置10, 30と同様な処理を行うようにすればよい。すなわち、変調部16, 35は、入力された信号に対して送信処理に対応する変調処理を行う。

受信装置については、図4及び図6に示したような再生装置50, 70においてディスク200からの信号を読み込むためのアンプ54, 74以前の構成を、受信手段に変更すればよい。例えば、受信手段の構成としては、搬送波処理部等が挙げられる。なお、このように、アンプ54, 74以降の構成を、受信手段に変更することによって受信装置とすることができ、アンプ54, 74の後段のブロック以降は、送信装置から送信されてデータの受信処理を行う。すなわち、

復調部 55, 75 は、入力された信号に対して受信処理に対応する復調処理を行う。

上述した送信装置及び受信装置は、無線放送、有線放送又はネットワークを介してデータの送受信がなされる。

上述の例では、記録媒体として、光ディスク、光磁気ディスク等のディスクを例に挙げて説明しているが、記録媒体は、ビデオテープ、半導体メモリ等であってもよい。この場合、記録手段や再生手段は、記録媒体に応じたものが用いられる。

以上の例によれば、広告や著作権管理情報等の必ず再生して欲しい情報を再生しないと、著作物の内容である本編又は本体部分に相当するコンテンツデータを正しく再生することができない。したがって、ユーザに対して、広告や著作権管理情報等を強制的に見せることができる。

以上の例によれば、ビデオ映像やテレビジョン放送の場合、広告が流れて（再生されて）初めて本編が見られるようになるので、広告効果を一層高めることができる。例えば、HDD (Hard Disc Drive) 付きのテレビジョン受像器等で広告映像をスキップ等の特殊再生をしようとする、と本編を正しく再生できなくなるので、ユーザは必ず広告を通常再生する必要がある。これによって、本例では、広告をユーザに対して確実に見せることができる。

広告データに暗号鍵を埋め込む方式として、デジタルデータの最下位ビットにウォーターマークを埋め込むような方式を採用した場合には、D/A 変換して得たアナログ信号を A/D 変換して再びデジタル信号に変換しても最下位のウォーターマークが完全に再現される可能性は低い、といった例からもわかるように、ウォーターマークを埋め込むことで、アナログ信号に変換した後に行われたコピー動作によってコンテンツデータの本編部分が再生されない方式にすることもできる。これにより、アナログ信号に変換してコピーされた場合には、コピーされたデータのうちの本編とされるコンテンツデータを再生することができなくなり、その一方で、広告部分のデータのみが再生されるようになる。

ホームページよりコンテンツデータを入手するとき、操作部となるバナー広告をクリックしないと、コンテンツデータを入手することができないようにするこ

とで、ユーザに対してバナー広告を必ず見せることができる。

以上のように、コンテンツに添付される広告の効果を絶大なものとすることができるので、これにより、ユーザは、広告付きコンテンツを安く購入することができるようになる。

以上例では、コンテンツデータが動画像データ（映像）の場合を例に挙げて説明したが、これに限定されるものではなく、例えば、コンテンツデータは、静止画像データ、オーディオデータ又はゲームデータであってもよい。また、コンテンツデータは、動画像データ、静止画像データ、オーディオデータ、ゲームデータ等の内、少なくとも1つを含むものであればよく、従って、広告データが含むコンテンツ秘匿用データによる秘匿対象は、例えば、楽曲データのプロモーションビデオのように、動画像データとオーディオデータとからなるコンテンツデータであってもよい。また、このようなコンテンツデータとして挙げられるデータの信号形態は、アナログ信号であってもよく、デジタル信号であってもよい。

上述の例では、ディスク200へのコンテンツデータと広告データとの信号記録形態は、時分割多重又は空間分割を前提として説明しているが、これに限定されるものではない。例えば、広告データを、ディスク200のデータ領域の最内周又は最外周側に記録することもできる。この場合には、上述の記録装置10，30や再生装置50，70は、それに対応した構成になる。例えば、記録装置10，30は、コンテンツデータと別にディスク200の最内周又は最外周側に広告データを記録するようにし、また、再生装置は、ディスク200の最内周又は最外周側に記録されている広告データを再生するようにする。これによって、ディスク200を再生したとき、コンテンツデータの再生に先立って広告データの再生が行われるようになる。トラックジャンプ等を行うことにより、広告データの再生を飛ばしてコンテンツデータの再生を行う操作をしたときには、広告データよりコンテンツ秘匿用データを抽出することができないことから、コンテンツデータの再生を阻止することができる。

上述の再生装置50，70は、デマルチプレクサ57，77を備え、ここでコンテンツデータと広告データとが分割されて、以降のブロックにおいて各種処理がなされる場合について説明しているが、デマルチプレクサ57，77を備える

ことに限定されるものではない。例えば、広告データから暗号鍵を抽出する暗号鍵抽出部 60 に、広告データとコンテンツデータとがそのまま入力されるようにして、所定のタイミングで広告データから暗号鍵を抽出するようにしてもよい。広告データの所定領域から暗号化に使用した暗号化用データを抽出する所定領域データ抽出部 78 に、広告データとコンテンツデータとがそのまま入力されるようにして、所定のタイミングで広告データから暗号化用データを抽出するようにしてもよい。

以上の例では、ディスク 200 等の記録媒体にコンテンツデータと広告データとが記録されている例を説明したが、以下に説明するように、ディスク 200 に暗号化されたコンテンツデータを記録しておき、コンテンツデータの暗号を解読するための暗号鍵を含む広告データをサーバ装置よりダウンロードするようにしてもよい。

すなわち、図 23 に示すように、コンテンツ制作会社 150 は、図 24 に示す記録装置 201 によってディスク 200 に暗号化したコンテンツデータを記録し、ユーザに対して配給する。ここで、コンテンツ制作会社 150 は、有料、無料又は通常価格より安い価格で記録媒体を配給する。広告制作会社 151 は、コンテンツデータを暗号化する際に用いた暗号鍵を含む広告データをサーバ装置 230 のホームページに公表する。ユーザは、図 25 に示す再生装置 201 でディスク 200 に暗号化された状態で記録されているコンテンツデータを再生する際、広告データをサーバ装置 220 よりネットワークを介して再生装置 201 にダウンロードし、この広告データを再生することによって暗号鍵を購入し、この暗号鍵でコンテンツデータの暗号を解読し再生する。

ここで、コンテンツ制作会社 150 の記録装置 201 について図 24 を用いて説明すると、この記録装置 201 は、入力端子 202 より入力されたコンテンツデータをエンコードするエンコーダ 203 と、エンコーダ 203 でエンコードされたコンテンツデータを暗号化する暗号化部 204 と、暗号化部 204 で暗号化されたコンテンツデータに対してエラー訂正符号化処理を施すエラー訂正符号化部 205 と、エラー訂正符号化部 205 でエラー訂正符号が付加されたコンテンツデータに対して変調処理を施す変調部 206 と、変調部 206 で変調されたコ

ンテンツデータを増幅するアンプ207と、ディスク200にコンテンツデータを記録する光学ヘッド208とを備える。入力端子209からは、コンテンツデータを暗号化するための暗号鍵が入力され、この暗号鍵は、暗号化部204に入力される。

以上のような記録装置201は、入力端子202よりコンテンツデータが入力され、入力端子209より暗号鍵が入力されると、先ず、エンコーダ203でコンテンツデータを上述したMPEG2等の方式でエンコードする。次いで、暗コード処理されたコンテンツデータは、暗号化部204に入力される。暗号化部204は、入力端子209より入力された暗号鍵が入力され、エンコード処理されたコンテンツデータを暗号鍵を用いて暗号化し、暗号化されたコンテンツデータをエラー訂正符号化部205に出力する。エラー訂正符号化部205は、入力されたコンテンツデータにエラー訂正符号化処理を施し、変調部206に出力し、変調部206は、エラー訂正符号化処理がなされたコンテンツデータに対して変調処理を施し、次いでアンプ207は、ディスク200に記録するコンテンツデータを増幅し、光学ヘッド208は、記録すべきコンテンツデータに対して記録処理を施して、ディスク200にコンテンツデータを記録する。

かくして、暗号化されたコンテンツデータが記録されたディスク200は、パッケージ化あされた後にユーザに対して配給される。

次に、ユーザが購入等したディスク200を再生する再生装置211について、図25を参照して説明すると、この再生装置211は、ディスク200より光ビームを照射してディスク200に記録されているコンテンツデータを読み出す光学ヘッド212と、光学ヘッド212より入力されたコンテンツデータを増幅し、RF信号等を抽出するRFアンプ213と、RFアンプ213より入力されたコンテンツデータに対して復調処理を施す復調部214と、復調されたコンテンツデータのエラー訂正処理を施すエラー訂正部215と、エラー訂正部215でエラー訂正されたコンテンツデータの暗号を解読する暗号解読部216と、暗号解読されたコンテンツデータを出力するモニタ217、スピーカ218とを備える。

再生装置211は、サーバ装置230よりダウンロードした広告データ等を保存する記憶部219と、記憶部219にデータを記録する共に記憶部219に保

存されているデータを読み出す磁気回路 220 と、磁気回路 220 で読み出したデータを復調する復調部 221 と、復調部 221 で復調されたデータのエラー訂正処理を施すエラー訂正部 222 と、エラー訂正部 222 でエラー訂正処理が施された広告データ等から暗号鍵を抽出する抽出部 223 とを備える。更に、再生装置 211 は、サーバ装置 230 に対してデータを送信する送信部 224 と、サーバ装置から送信されたデータを受信する受信部 225 と、ユーザによって操作される操作部 226 と、操作部 226 からの入力に応じて装置全体を制御する制御部 227 とを備える。

ここで、再生装置 211 がアクセスするサーバ装置 230 には、図 26 に示すようなホームページ 231 が開設されている。このホームページ 231 は、コンテンツデータに関連するバナー広告 1A～1C とバナー広告 2A～2D が設けられている。これらバナー広告 1A～1C, 2A～2D は、再生装置 211 のモニタ 217 にホームページ 231 が表示されているとき、操作部 226 によりクリックされると、コンテンツデータに関連するデータ、例えば広告データ、プロモーションデータを新たなウェブページを開くようになっている。ここで、広告データ等は、コンテンツデータを暗号化したときの暗号鍵が含まれている。

再生装置 211 は、ディスク 200 に暗号化されて記録されているコンテンツデータを再生するにあたっては、先ず、サーバ装置 230 よりコンテンツデータをダウンロードする必要がある。このため、先ず、再生装置 211 は、操作部 226 を操作することによって、例えばディスク 200 の収納ケース等に記録されている所定の URL を入力し、サーバ装置 230 にアクセスし、モニタ 217 にホームページ 231 を表示する。ユーザは、再生しようとするコンテンツデータのバナー広告 1A～1C, 2A～2D を操作部 226 でクリックする。すると、再生装置 211 は、送信部 224 より送信要求を送信し、これを受信したサーバ装置 230 より、クリックしたバナー広告に対応した表示データを受信し、記憶部 219 に保存する。再生装置 211 は、モニタ 217 にウェブページを表示する。ここで、再生装置 211 は、このウェブページよりコンテンツデータの暗号鍵が含まれた広告データをダウンロードする。この広告データ等は、記憶部 219 に保存される。

ここで、ユーザがディスク 200 を装着部に装着し、ディスク 200 に暗号化されて記録されているコンテンツデータの再生を開始しようとする、制御部 227 は、広告データの再生を開始する。すなわち、図 27 に示すように、ステップ S101 において、磁気回路 220 は、記憶部 219 より広告データを読み出す。ステップ S102 において、再生装置 211 は、広告データの復調処理を行い、次いで、エラー訂正処理を施し、モニタ 217 やスピーカ 218 より出力する。このとき、抽出部 223 は、エラー訂正された広告データよりコンテンツデータの暗号化に用いられた暗号鍵を抽出する。

ステップ S103 において、制御部 226 は、抽出部 223 が暗号鍵を抽出できたかどうかを判断し、暗号鍵を抽出することができたときステップ S104 に進み、暗号鍵を抽出することができなかったとき、ステップ S106 に進む。

暗号鍵を抽出部 223 で抽出することができ、ディスク 200 に暗号化されて記録されているコンテンツデータの再生が開始されると、ステップ S104 において、コンテンツデータは、RF アンプ 213 で増幅され、復調部 214 で復調され、エラー訂正部 215 でエラー訂正処理がなされる。そして、ステップ S104 において、エラー訂正がなされたコンテンツデータは、暗号解読部 216 で、抽出部 223 より入力された暗号鍵で暗号解読され、モニタ 217 やスピーカ 218 に出力される。

また、ステップ S103 において、抽出部 223 で暗号鍵を抽出することができなかった状態でディスク 200 に暗号化されて記録されているコンテンツデータの再生を行うとき、制御部 227 は、再生しようとするコンテンツデータが暗号解読が必要であるか、すなわちコンテンツデータの再生に先立って広告データの再生が必要であるかを判断し、必要であるとき、ステップ S107 に進み、必要でないとき、ステップ S101 に戻る。

ステップ S107 において、制御部 227 は、例えばモニタ 217 にコンテンツデータの再生に先立って広告データの再生が必要である等の警告表示を行う。

なお、サーバ装置 230 は、暗号鍵を含む広告データをダウンロードするとき、課金処理を施すようにしてもよい。これによって、本システムでは、ディスク 200 をユーザに対して頒布するとき、無料にしたり、通常価格より安くする

ことができる。

ここで、広告データへの暗号鍵の埋め込みは、上記図 7 に示すように、広告データの所定フレーム画面 P の所定のラインデータ d をそのまま暗号化用データとして用いてもよく、また、上記図 8 に示すように、広告データの所定フレーム画面 P 全体のデータを暗号化用データとして用いてもよく、更に、上記図 9 に示すように、広告データの所定フレームの信号中の帰線消去期間中、すなわち表示画面 P の外側に位置する部分に暗号鍵 d を埋め込むようにしてもよく、更にまた、全フレームに亘って該各フレーム画面 F の一部にデータ（暗号鍵の一部）d を埋め込むようにしてもよく、更にまた、上記図 11 及び図 12 に示すように、画像信号中の下位データに暗号鍵をウォーターマークを用いて埋め込むようにしてもよい。

コンテンツデータの暗号化の方法としては、上記図 14 に示すように、広告 1 ～広告 4 の 4 個の広告データに埋め込まれる暗号鍵の一又は複数を用いてコンテンツデータを暗号化するようにしてもよく、また、上記図 15 に示すように、広告 1 ～広告 4 の 4 個の広告データに埋め込まれる暗号鍵を用いて、一方向性関数である H a s h 関数により 1 つの暗号鍵を生成して、その暗号鍵に基づいてコンテンツデータを暗号化するようにしてもよく、更に、上記図 16 に示すように、広告データを他の広告データの暗号鍵に基づいて暗号化するようにしてもよく、更にまた、上記図 17 に示すように、広告 1 ～広告 4 の各広告データに埋め込まれる暗号鍵により、4 分割されるコンテンツデータ A のそれぞれ対応される領域 A (1) ～領域 (4) を暗号化するようにしてもよい。

以上の例によれば、広告や著作権管理情報等の必ず再生して欲しい情報を再生しないと、コンテンツデータ（本編又は本体）を正しく再生することができない。したがって、ユーザ対して、広告や著作権管理情報等を強制的に見せることができる。

以上の例では、コンテンツデータをディスク 200 で提供し、広告データをサーバ装置 230 よりダウンロードする例を説明したが、本発明は、広告データ等の第 2 のコンテンツデータを光ディスク、光磁気ディスク、磁気ディスク、半導体メモリ等の記録媒体で配給するようにしてもよく、映画、ゲーム、音楽等の第

1 のコンテンツデータをサーバ装置 230 よりダウンロードするようにしてもよい。、第1のコンテンツデータや第2のコンテンツデータは、無線放送、有線放送等を介して配信するようにしてもよい。

産業上の利用可能性

本発明によれば、所定データを再生してコンテンツ秘匿用データを入手して、入手したコンテンツ秘匿用データに基づいてコンテンツの秘匿を解除して再生するので、コンテンツデータに先行して必ず所定データが再生されるようになる。よって、データ記録媒体は、所定データが広告であるときには、コンテンツデータに先行して広告データを再生させることができるので、広告効果をより高めることができる。

請求の範囲

1. コンテンツデータからなる第1のデータを再生する際に上記第1のデータに先だって再生される位置に、上記コンテンツデータを秘匿するためのコンテンツ秘匿用データが埋めこまれた第2のデータが記録された記録媒体。
2. 上記第2のデータは少なくともひとつの広告データである請求の範囲第1項記載の記録媒体。
3. 上記第2のデータは、複数の広告データからなり、上記コンテンツ秘匿データは上記複数の広告データに分散されて埋め込まれている請求の範囲第1項記載の記録媒体。
4. 上記第2のデータは、複数の広告データからなり、上記複数の広告データにはそれぞれ暗号化処理が施されているとともに上記複数の広告データのうち或る広告データには残りの広告データのうちのひとつの広告データに施されている暗号処理を解読するための鍵データが埋め込まれており、上記複数の広告データのうち最後に再生される広告データに上記コンテンツ秘匿用データが埋め込まれている請求の範囲第1項記載の記録媒体。
5. 上記コンテンツ秘匿用データは、上記第2のデータの帰線消去期間中に埋め込まれている請求の範囲第1項記載の記録媒体。
6. 第1のデータと第2のデータとが記録されるとともに、上記第2のデータは上記第1のデータを再生する際に上記第1のデータよりも先だって読み出される位置に記録され、上記第1のデータは上記第2のデータから抜き出されたデータを用いて暗号化処理が施されて記録された記録媒体。
7. 上記第2のデータは少なくともひとつの広告データである請求の範囲第6項記載の記録媒体。
8. 上記第2のデータから抜き出されたデータは、上記広告データの所定のフレームの所定ラインデータである請求の範囲第6項記載の記録媒体。
9. 上記第2のデータから抜き出されたデータは、上記広告データの所定のフレームのデータである請求の範囲第6項記載の記録媒体。
10. 供給された第2のデータにコンテンツデータからなる第1のデータを秘匿

するためのコンテンツ秘匿用データを埋め込み、

上記第1のデータを上記コンテンツ秘匿用データを用いて秘匿処理を施し、

上記コンテンツ秘匿用データが埋め込まれた上記第2のデータと上記秘匿処理が施された上記コンテンツデータとにエンコード処理を施して記録媒体に記録する記録媒体の記録方法。

11. 上記方法は、上記コンテンツ秘匿用データが埋め込まれた上記第2のデータと上記秘匿処理が施された上記コンテンツデータを多重化し、上記多重化されたデータに上記エンコード処理を施す請求の範囲第10項記載の記録媒体の記録方法。

12. 上記第2のデータは少なくともひとつの広告データである請求の範囲第10項記載の記録媒体の記録方法。

13. 上記第2のデータは、複数の広告データからなり、上記コンテンツ秘匿データは上記複数の広告データに分散されて埋め込まれる請求の範囲第10項記載の記録媒体の記録方法。

14. 上記コンテンツ秘匿用データは、上記第2のデータの帰線消去期間中に埋め込まれている請求の範囲第10項記載の記録媒体の記録方法。

15. 上記方法は、更に上記第1のデータと上記コンテンツ秘匿用データが埋め込まれた上記第2のデータとの各々に圧縮処理を施し、上記圧縮処理が施された上記第1のデータと上記第2のデータに上記秘匿処理が施される請求の範囲第10項記載の記録媒体の記録方法。

16. 上記方法は、上記コンテンツ秘匿データが埋め込まれた上記第2のデータは上記第1のデータに先だって読み出される上記記録媒体上の位置に記録される請求の範囲第10項記載の記録媒体の記録方法。

17. 供給された第2のデータから抜き出したデータを用いてコンテンツデータからなる第1のデータに暗号化処理を施し、

上記第2のデータと上記暗号化処理が施された上記第1のデータとにエンコード処理を施して記録媒体に記憶する記録媒体の記録方法。

18. 上記方法は、上記第2のデータと上記暗号化処理が施された上記第1のデータとを多重化し、上記多重化されたデータに上記エンコード処理を施す請求の

範囲第 1 7 項記載の記録媒体の記録方法。

19. 上記第 2 のデータは少なくともひとつの広告データである請求の範囲第 1 7 項記載の記録媒体の記録方法。

20. 上記第 2 のデータから抜き出されたデータは、上記広告データの所定のフレームの所定ラインデータである請求の範囲第 1 7 項記載の記録媒体の記録方法。

21. 上記第 2 のデータから抜き出されたデータは、上記広告データの所定のフレームのデータである請求の範囲第 1 7 項記載の記録媒体の記録方法。

22. 上記方法は、上記コンテンツ秘匿データが埋めこまれた上記第 2 のデータは上記第 1 のデータに先だって読み出される上記記録媒体上の位置に記録される請求の範囲第 1 7 項記載の記録媒体の記録方法。

23. 供給された複数の第 2 のデータに、コンテンツのデータからなる第 1 のデータに暗号化処理を施すための暗号鍵データを各々埋めこみ、

上記第 2 のデータに埋めこまれた暗号鍵データに基づいて上記第 1 のデータの少なくとも一部の領域に秘匿処理を施し、

上記コンテンツ秘匿用データが埋めこまれた上記第 2 のデータと上記秘匿処理が施された上記コンテンツデータとにエンコード処理を施して記録するデータ記録方法。

24. 上記複数の第 2 のデータは、各々広告データからなり、上記方法は上記複数の広告データから読み出された上記複数の暗号鍵データを用いてコンテンツ秘匿用データを生成し、上記生成されたコンテンツ秘匿用データに基づいて上記第 1 のデータに秘匿処理を施す請求の範囲第 2 3 項記載のデータ記録方法。

25. 上記複数の第 2 のデータは、各々広告データからなり、上記方法は上記複数の広告データから読み出された上記複数の暗号鍵データを用いて上記第 1 のデータの複数の各々の領域に秘匿処理を施す請求の範囲第 2 3 項記載のデータ記録方法。

26. コンテンツデータからなる第 1 のデータを再生する際に上記第 1 のデータに先だって再生される位置に、上記コンテンツデータを秘匿するためのコンテンツ秘匿用データが埋めこまれた第 2 のデータが記録された記録媒体から読み出された上記第 2 のデータから上記コンテンツ秘匿データを抽出し、

上記抽出された上記コンテンツ秘匿データを用いて上記記録媒体から読み出された上記第 1 のデータに施されている暗号を解読し、

上記第 2 のデータに引き続いて上記解読された上記第 1 のデータを出力する記録媒体の再生方法。

27. 上記方法は、上記記録媒体から読み出された上記第 2 のデータを一旦バッファメモリに取りこみ、上記バッファメモリに取りこまれた上記第 2 のデータから上記コンテンツ秘匿用データを抽出する請求の範囲第 26 項記載の記録媒体の再生方法。

28. 上記方法は、上記記録媒体から上記第 2 のデータを読み出せなかったとき、または上記第 2 のデータから上記コンテンツ秘匿データが抽出できなかったときの何れか一方の場合には上記第 1 のデータの再生を中止する請求の範囲第 26 項記載の記録媒体の再生方法。

29. 上記方法は、上記第 2 のデータが特殊再生されたときには上記第 1 のデータの暗号解読処理を中止する請求の範囲第 26 項記載の記録媒体の再生方法。

30. 第 1 のデータと第 2 のデータとが記録されるとともに、上記第 2 のデータは上記第 1 のデータを再生する際に上記第 1 のデータよりも先だって読み出される位置に記録され、上記第 1 のデータは上記第 2 のデータから抜き出されたデータを用いて暗号化処理が施されて記録された記録媒体から上記第 2 のデータが読み出され、

上記読み出された上記第 2 のデータの所定の領域のデータを抜き出し、

上記抜き出されたデータを用いて上記記録媒体から読み出された上記第 1 のデータに施されている暗号を解読し、

上記第 2 のデータに引き続いて上記解読された上記第 1 のデータを出力する記録媒体の再生方法。

31. 上記方法は、上記記録媒体から上記第 2 のデータを読み出せなかったとき、または上記第 2 のデータから上記所定の領域のデータが抜き出せなかったときの何れか一方の場合には上記第 1 のデータの再生を中止する請求の範囲第 30 項記載の記録媒体の再生方法。

32. 上記方法は、上記第 2 のデータが特殊再生されたときには上記第 1 のデー

タの暗号解読処理を中止する請求の範囲第30項記載の記録媒体の再生方法。

33. 供給された第2のデータにコンテンツデータからなる第1のデータを秘匿するためのコンテンツ秘匿用データを埋め込み、

上記第1のデータを上記コンテンツ秘匿用データを用いて秘匿処理を施し、

上記コンテンツ秘匿用データが埋め込まれた上記第2のデータと上記秘匿処理が施された上記コンテンツデータとにエンコード処理を施して送信するデータの送信方法。

34. 上記方法は、上記コンテンツ秘匿用データが埋め込まれた上記第2のデータと上記秘匿処理が施された上記コンテンツデータを多重化し、上記多重化されたデータに上記エンコード処理を施す請求の範囲第33記載のデータの送信方法。

35. 上記第2のデータは少なくともひとつの広告データである請求の範囲第33項記載のデータの送信方法。

36. 上記第2のデータは、複数の広告データからなり、上記コンテンツ秘匿データは上記複数の広告データに分散されて埋め込まれる請求の範囲第33項記載のデータの送信方法。

37. 上記コンテンツ秘匿用データは、上記第2のデータの帰線消去期間中に埋め込まれている請求の範囲第33項記載のデータの送信方法。

38. 上記方法は、更に上記第1のデータと上記コンテンツ秘匿用データが埋め込まれた上記第2のデータとの各々に圧縮処理を施し、上記圧縮処理が施された上記第1のデータと上記第2のデータに上記秘匿処理が施される請求の範囲第33項記載のデータの送信方法。

39. 供給された第2のデータから抜き出したデータを用いてコンテンツデータからなる第1のデータに暗号化処理を施し、

上記第2のデータと上記暗号化処理が施された上記第1のデータとにエンコード処理を施して送信するデータの送信方法。

40. 上記方法は、上記第2のデータと上記暗号化処理が施された上記第1のデータとを多重化し、上記多重化されたデータに上記エンコード処理を施す請求の範囲第39項記載のデータの送信方法。

41. 上記第2のデータは少なくともひとつの広告データである請求の範囲第3

9 項記載のデータの送信方法。

4 2 . 上記第 2 のデータから抜き出されたデータは、上記広告データの所定のフレームの所定ラインデータである請求の範囲第 3 9 項記載のデータの送信方法。

4 3 . 上記第 2 のデータから抜き出されたデータは、上記広告データの所定のフレームのデータである請求の範囲第 3 9 項記載のデータの送信方法。

4 4 . コンテンツデータからなる第 1 のデータを再生する際に上記第 1 のデータに先だって再生され、上記コンテンツデータを秘匿するためのコンテンツ秘匿用データが埋めこまれた第 2 のデータを含むデータの上記第 2 のデータから上記コンテンツ秘匿データを抽出し、

上記抽出された上記コンテンツ秘匿データを用いて上記第 1 のデータに施されている暗号を解読し、

上記第 2 のデータに引き続いて上記解読された上記第 1 のデータを出力するデータ再生方法。

4 5 . 上記方法は、上記第 2 のデータを一旦バッファメモリに取りこみ、上記バッファメモリに取りこまれた上記第 2 のデータから上記コンテンツ秘匿用データを抽出する請求の範囲第 4 4 項記載のデータ再生方法。

4 6 . 上記方法は、上記第 2 のデータが特殊再生されたときには上記第 1 のデータの暗号解読処理を中止する請求の範囲第 4 4 項記載のデータ再生方法。

4 7 . 上記方法は、上記第 2 のデータを読み出せなかったとき、または上記第 2 のデータから上記コンテンツ秘匿データが抽出できなかったときの何れか一方の場合には上記第 1 のデータの再生を中止する請求の範囲第 4 4 項記載のデータ再生方法。

4 8 . 上記方法は、上記第 2 のデータが特殊再生されたときには上記第 1 のデータの暗号解読処理を中止する請求の範囲第 4 4 項記載のデータ再生方法。

4 9 . 第 1 のデータと第 2 のデータとを含み、上記第 2 のデータは上記第 1 のデータを再生する際に上記第 1 のデータよりも先だって読み出される位置に配され、上記第 1 のデータは上記第 2 のデータから抜き出されたデータを用いて暗号化処理が施されているデータの上記第 2 のデータの所定の領域のデータを抜き出し、

上記抜き出されたデータを用いて上記第 1 のデータに施されている暗号を解読

し、

上記第 2 のデータに引き続いて上記解読された上記第 1 のデータを出力するデータ再生方法。

50. 上記方法は、上記第 2 のデータを読み出せなかったとき、または上記第 2 のデータから上記所定の領域のデータが抜き出せなかったときの何れか一方の場合には上記第 1 のデータの再生を中止する請求の範囲第 49 項記載のデータ再生方法。

51. 上記方法は、上記第 2 のデータが特殊再生されたときには上記第 1 のデータの暗号解読処理を中止する請求の範囲第 49 項記載のデータ再生方法。

52. コンテンツデータからなる第 1 のデータがコンテンツ秘匿用データに基づいて暗号化処理が施されて記録された記録媒体の上記第 1 のデータを再生装置によって再生する際に、上記コンテンツ秘匿用データが埋めこまれた第 2 のデータをネットワークを介して上記再生装置に取りこみ、

上記取りこまれた上記第 2 のデータから上記コンテンツ秘匿データを抽出し、

上記抽出された上記コンテンツ秘匿データを用いて上記記録媒体から読み出された上記第 1 のデータに施されている暗号を解読し、

上記第 2 のデータに引き続いて上記解読された上記第 1 のデータを出力する再生方法。

53. 上記第 2 のデータは少なくともひとつの広告データである請求の範囲第 52 項記載の再生方法。

54. 上記方法は、上記第 2 のデータを一旦記憶部に取りこみ、上記記憶部に取りこまれた上記第 2 のデータから上記コンテンツ秘匿用データを抽出する請求の範囲第 52 項記載の再生方法。

55. 上記方法は、上記第 2 のデータから上記コンテンツ秘匿用データを抽出できなかったときには上記記録媒体から読み出された上記第 1 のデータに暗号解読処理が必要であるか否かを判別し、上記暗号解読処理が必要であると判別されたときには警告表示を行う請求の範囲第 52 項記載の再生方法。

56. 上記コンテンツ秘匿用データは、上記第 2 のデータの帰線消去期間中に埋め込まれている請求の範囲第 52 項記載の再生方法。

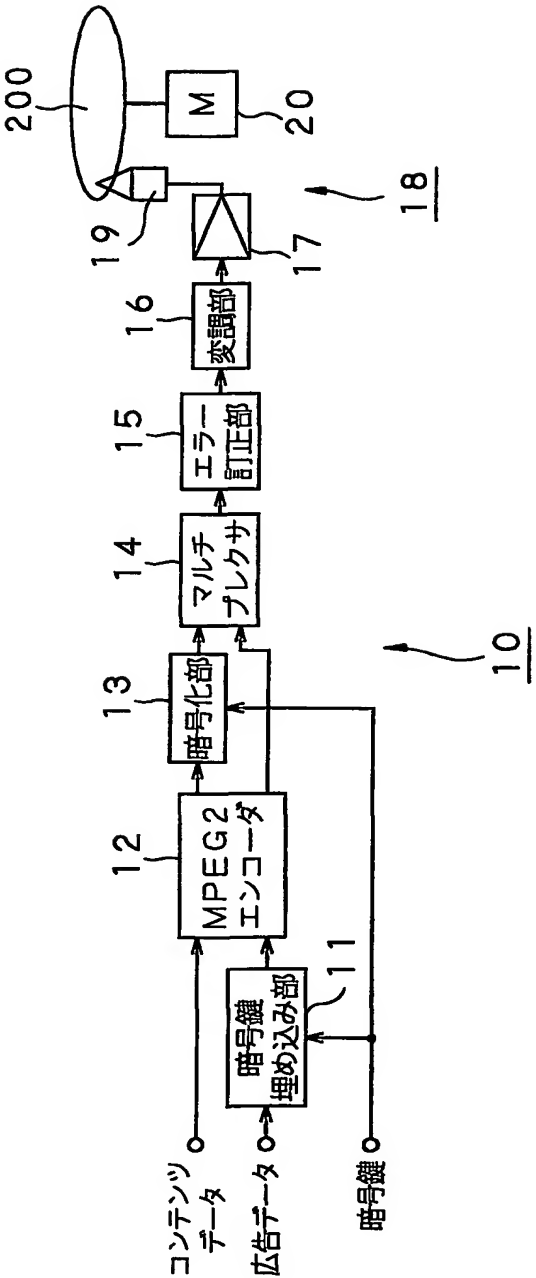
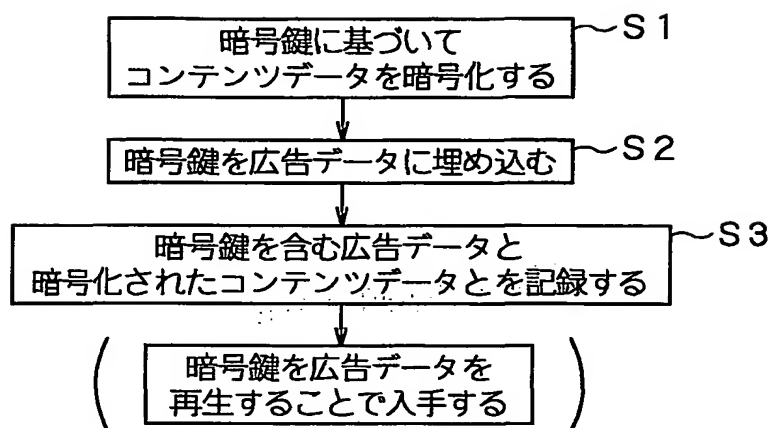


Fig. 1

THIS PAGE BLANK (USPTO)

2/21



Fi g.2

THIS PAGE BLANK (USPTO)

3/21

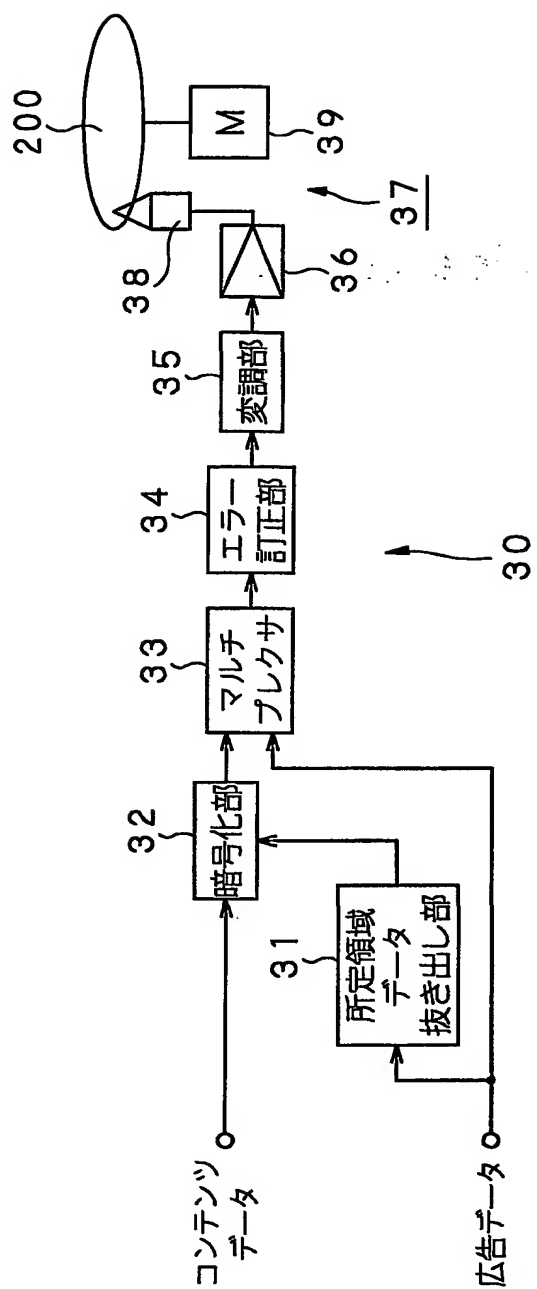
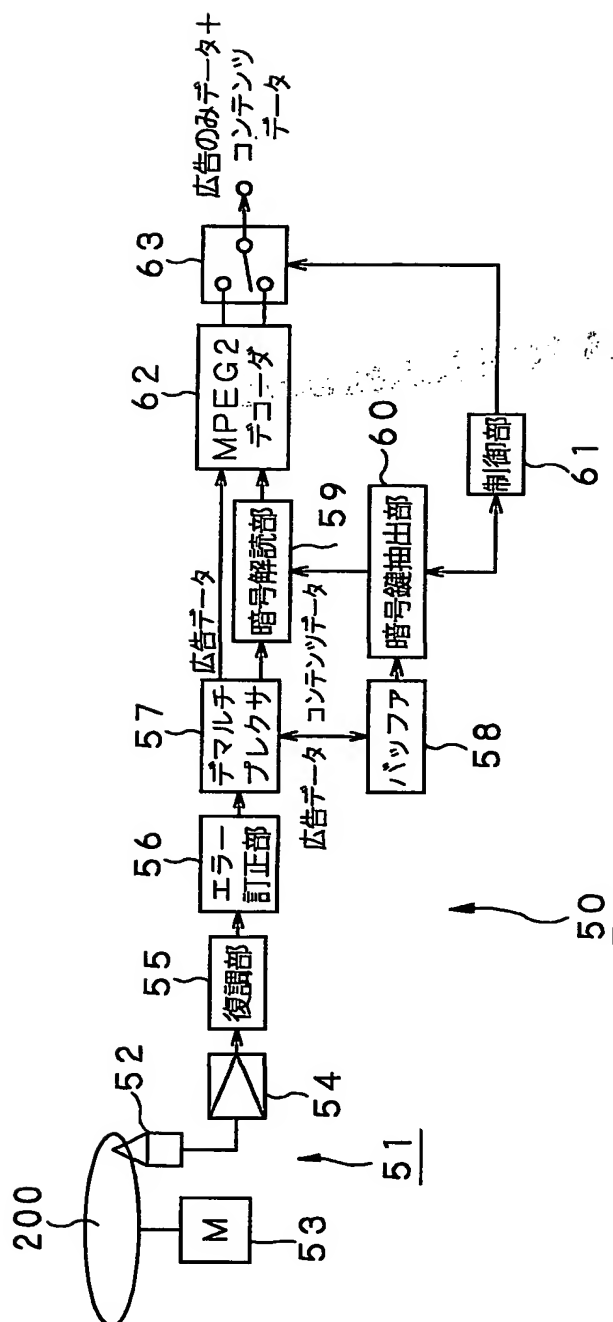


Fig. 3

THIS PAGE BLANK (USPTO)



4.
b0
-
L

THIS PAGE BLANK (USPTO)

5/21

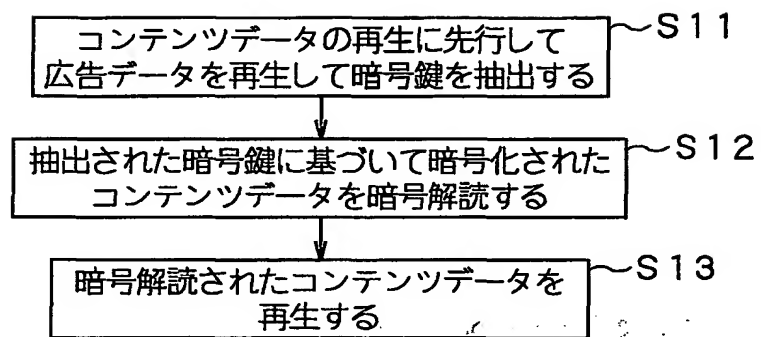


Fig. 5

THIS PAGE BLANK (USPTO)

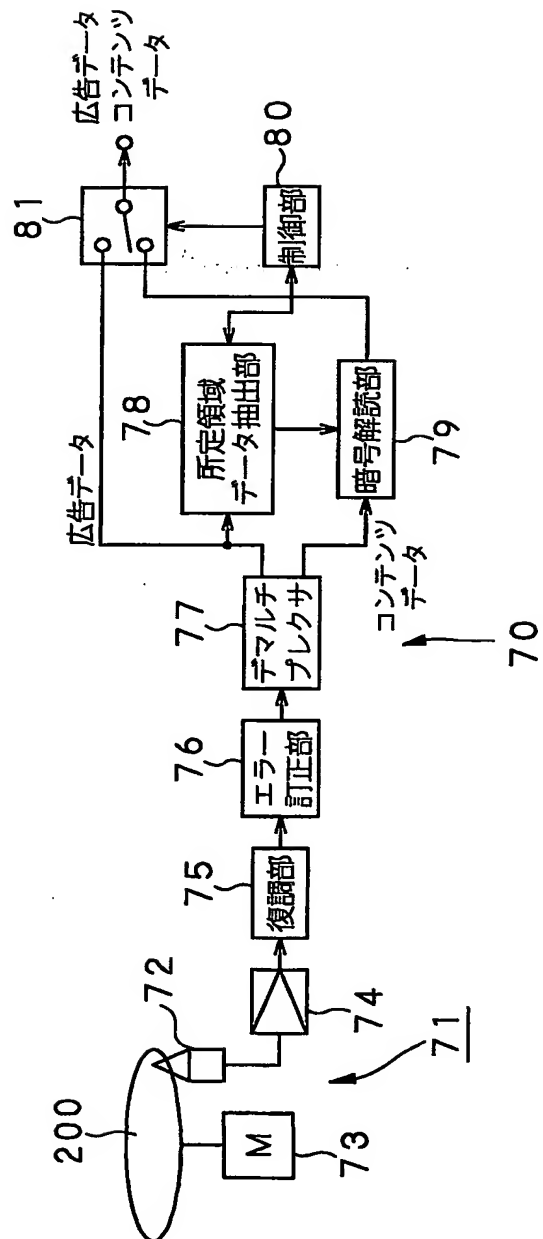
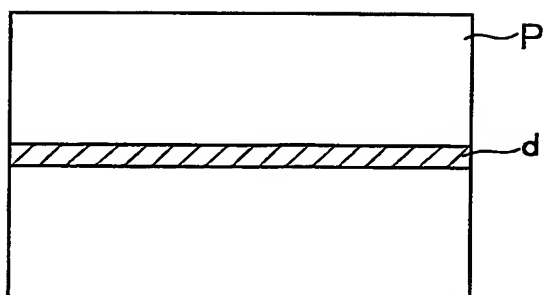


Fig. 6

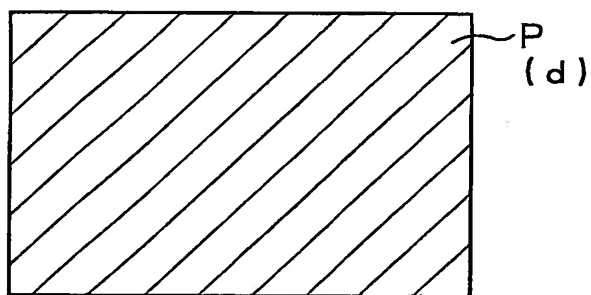
THIS PAGE BLANK (USPTO)

7/21



Fi g.7

FIG. 7 is a cross-sectional view of a device according to the present invention.



Fi g.8

THIS PAGE BLANK (USPTO)

8/21

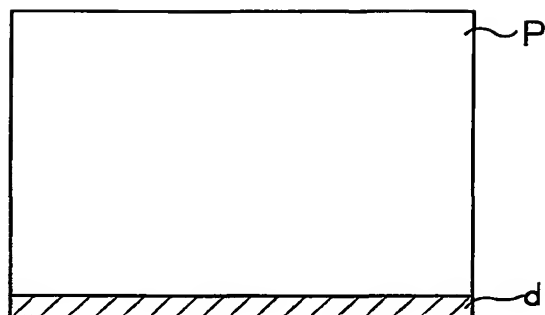


Fig. 9

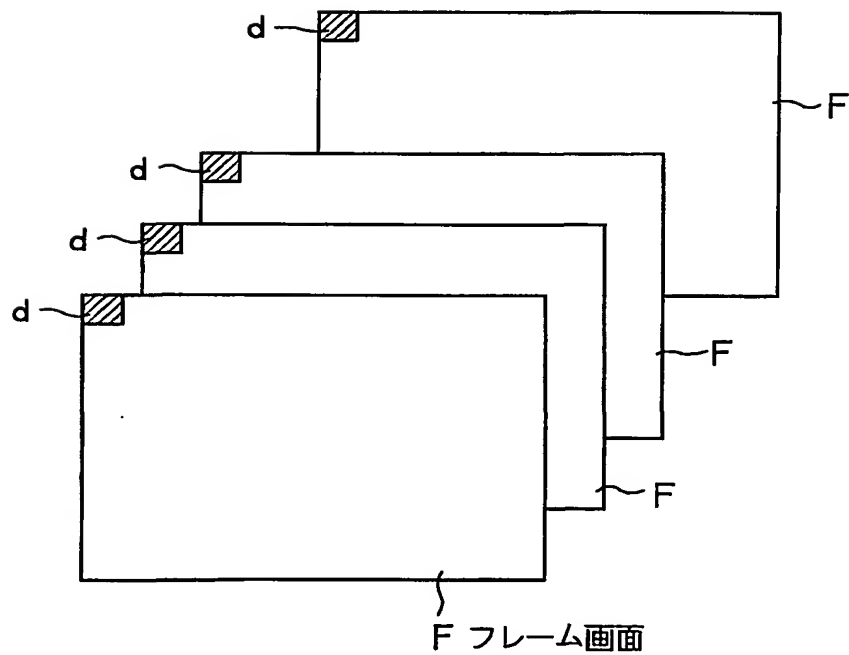
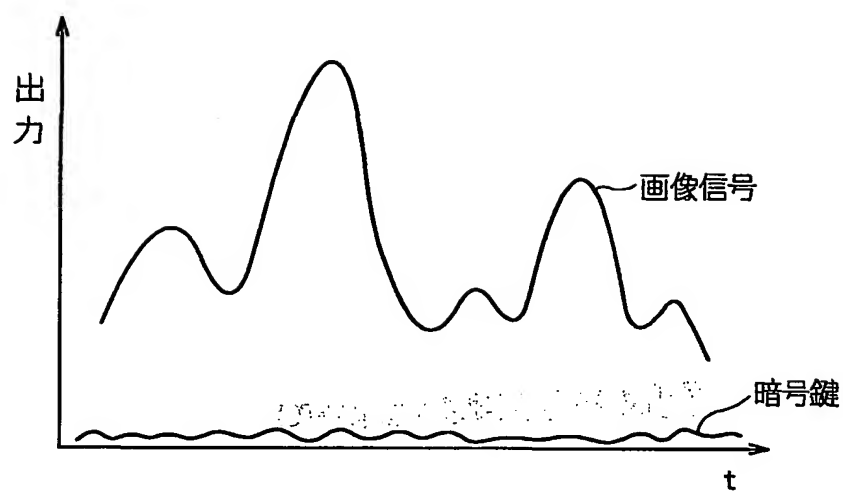


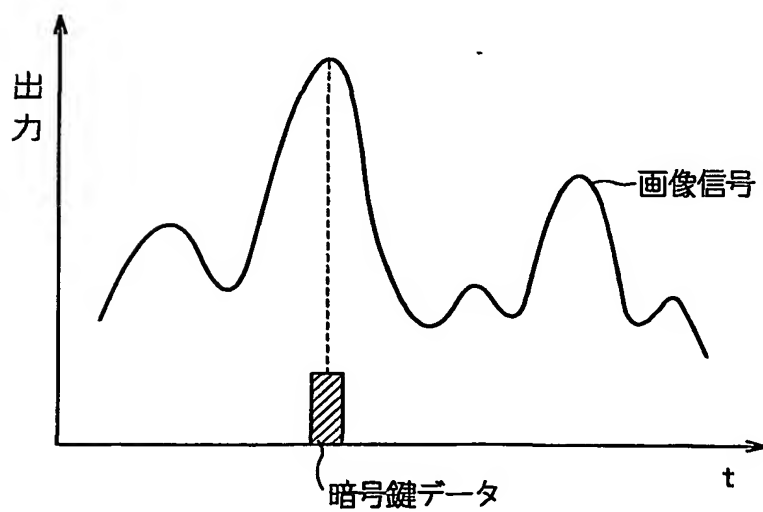
Fig. 10

THIS PAGE BLANK (USPTO)

9/21



Fi g.11



Fi g.12

THIS PAGE BLANK (USPTO)



Fi g.13

THIS PAGE BLANK (USPTO)

11/21

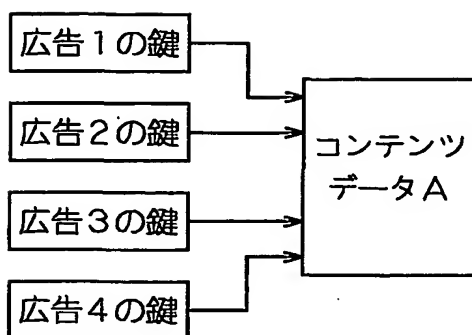


Fig.14

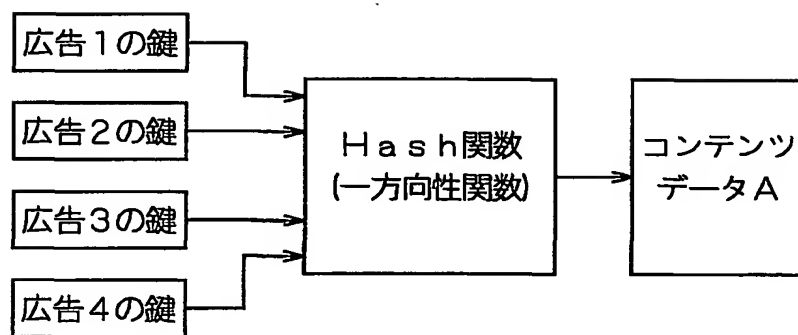


Fig.15

THIS PAGE BLANK (USPTO)

12/21

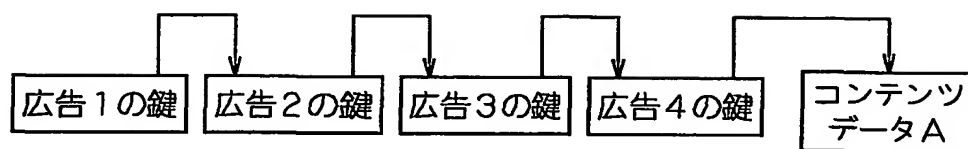


Fig. 16

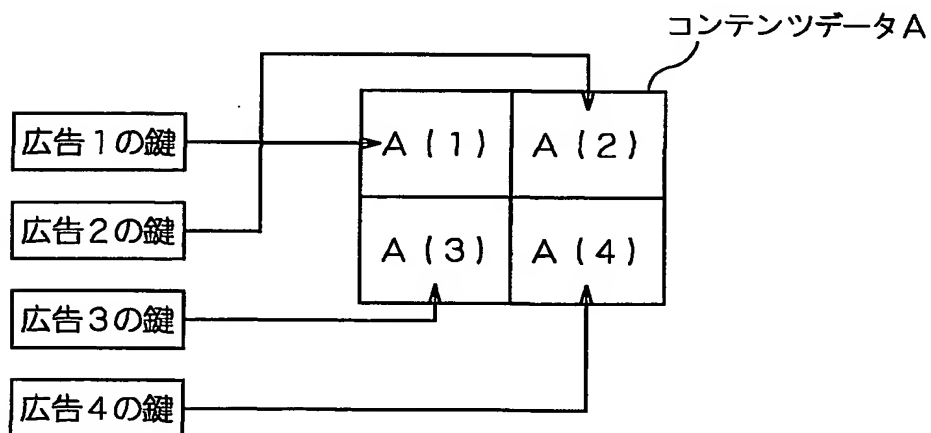


Fig. 17

THIS PAGE BLANK (USPTO)

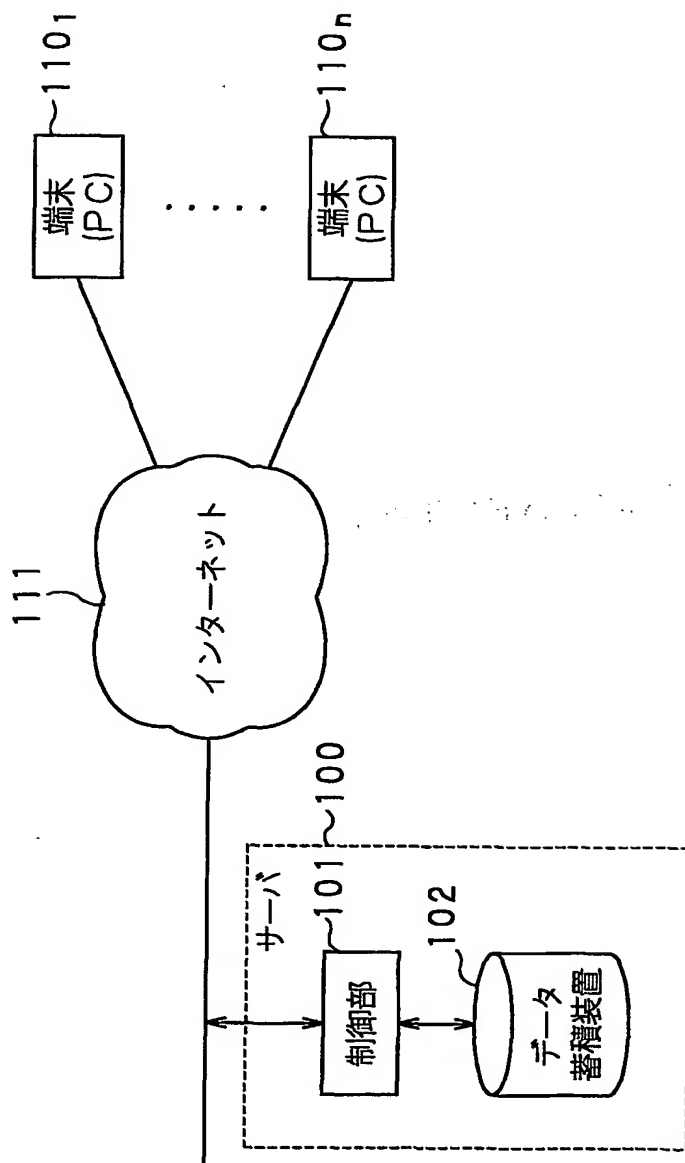


Fig. 18

THIS PAGE BLANK (USPTO)

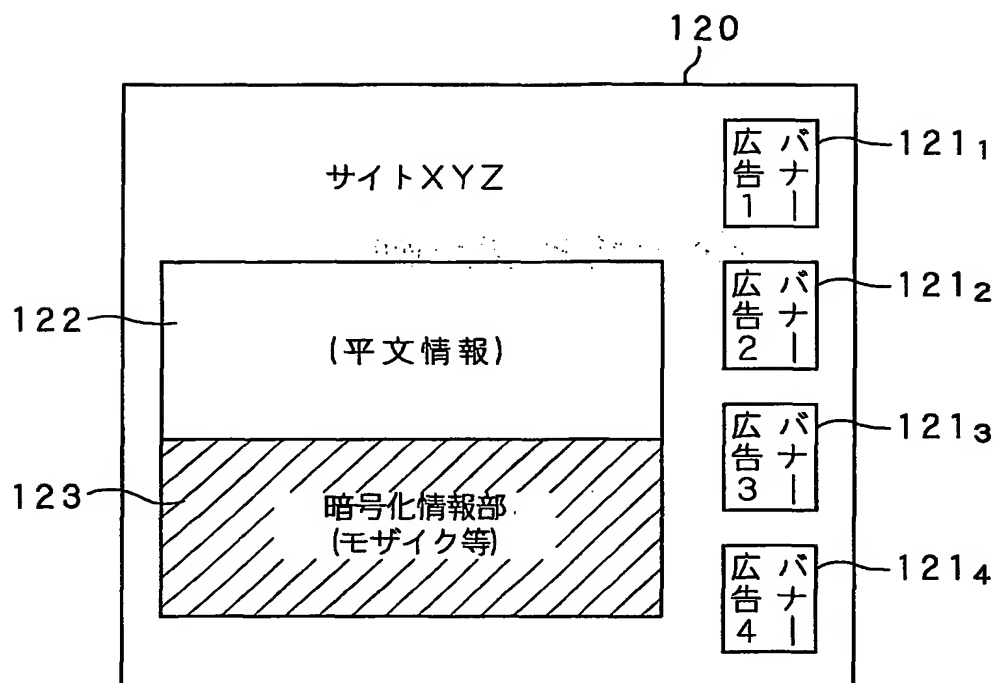
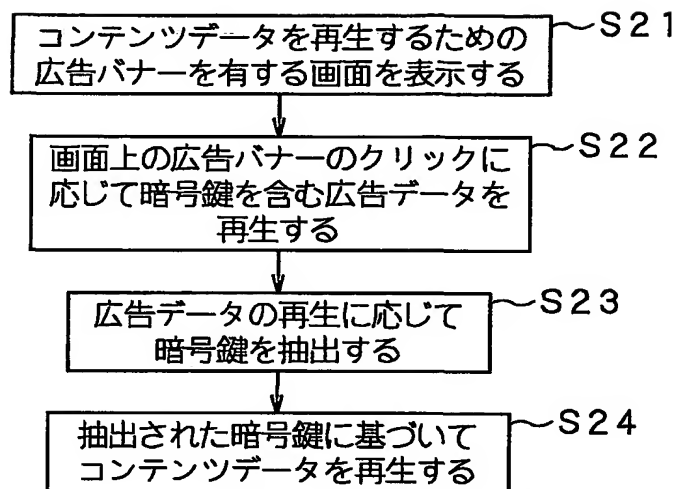


Fig. 19

THIS PAGE BLANK (USPTO)

15/21



Fi g.20

THIS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)

16/21

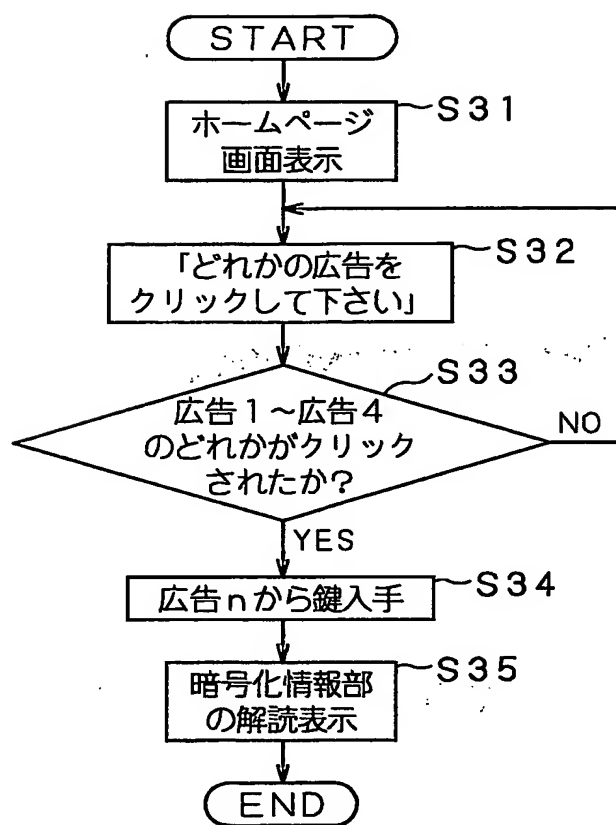
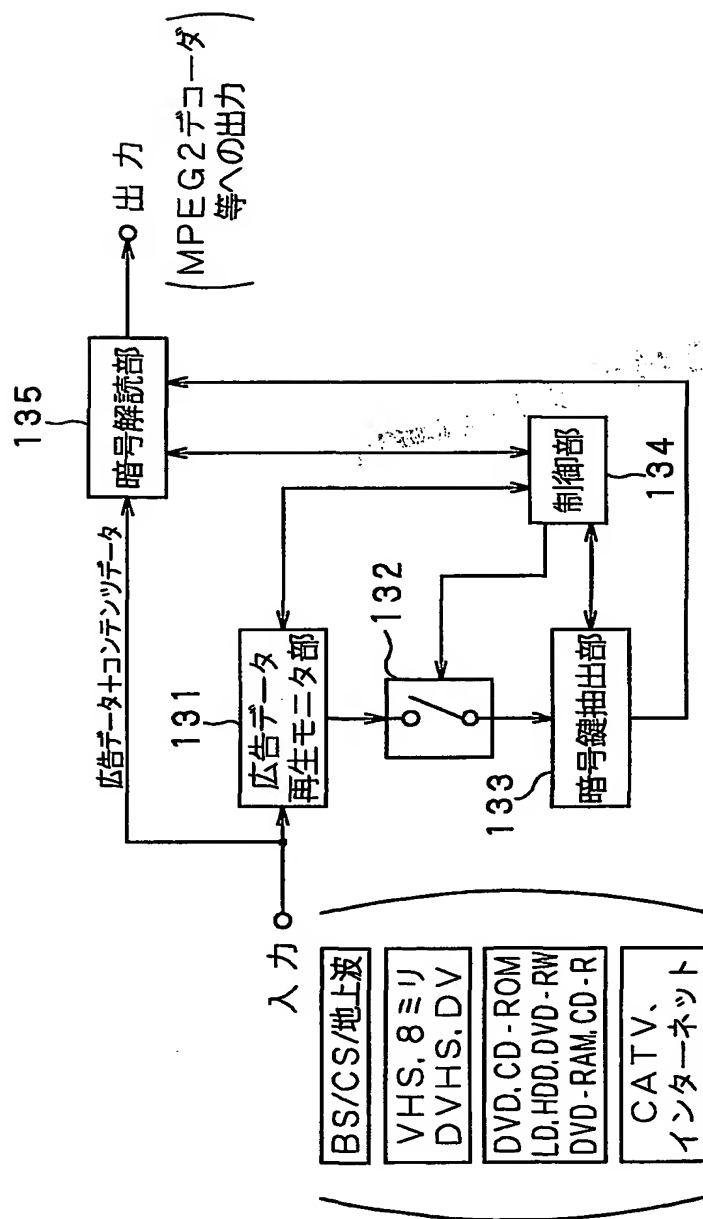


Fig.21

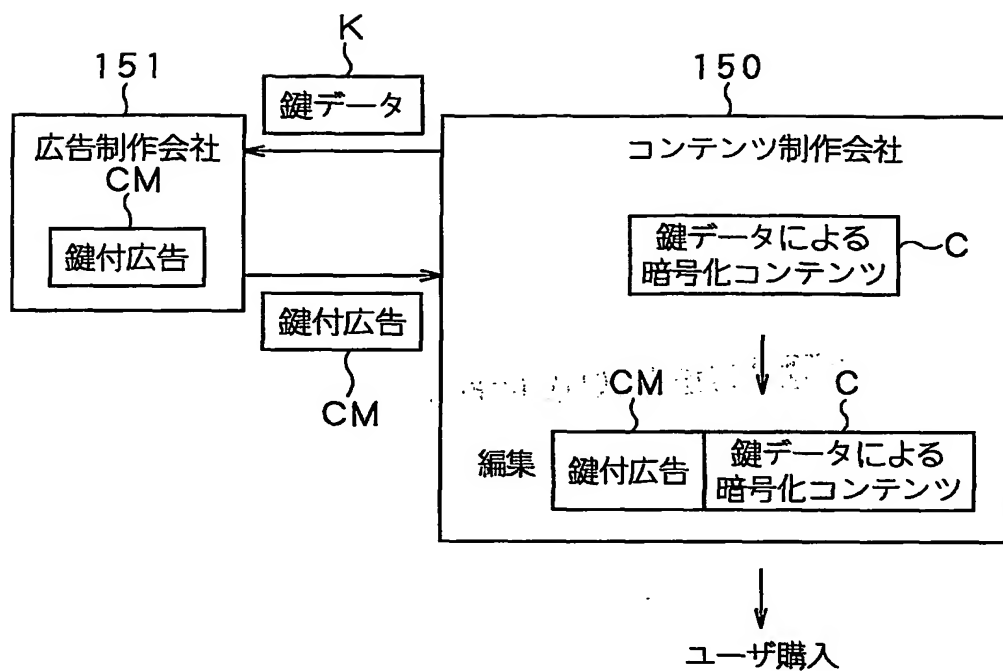
THIS PAGE BLANK (USPTO)



Fi. 2.2

THIS PAGE BLANK (USPTO)

18/21



Fi g.23

THIS PAGE BLANK (USPTO)

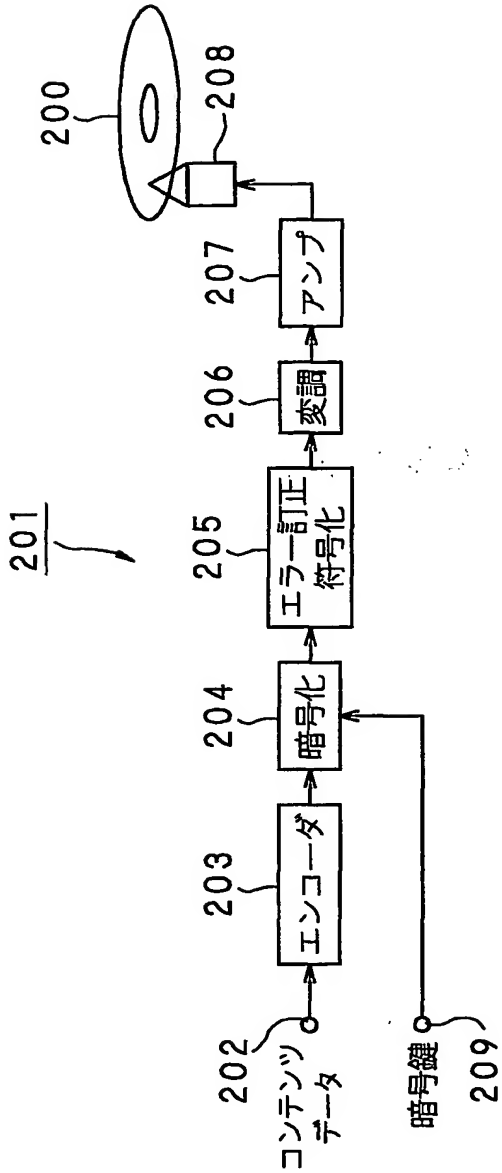
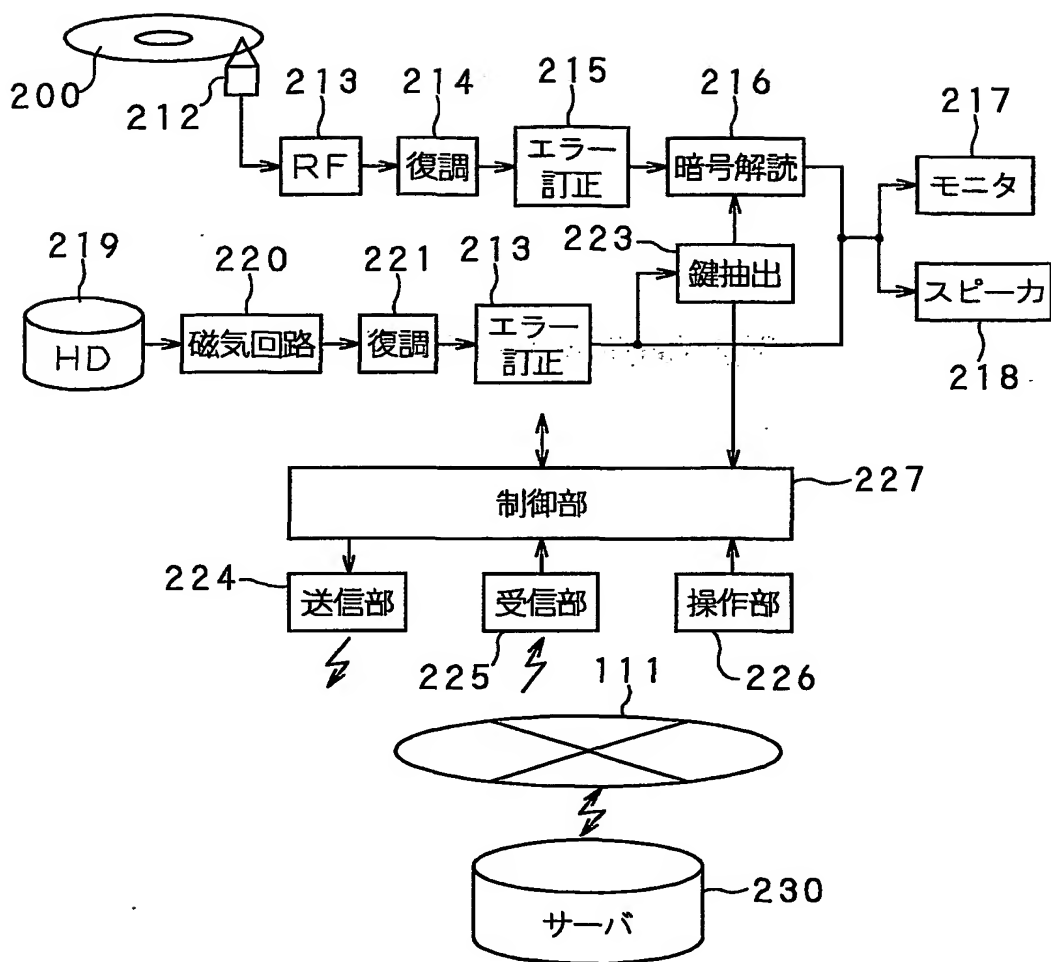


Fig. 24

THIS PAGE BLANK (USPTO)

20/21



Fi g.25

THIS PAGE BLANK (USPTO)

21/21

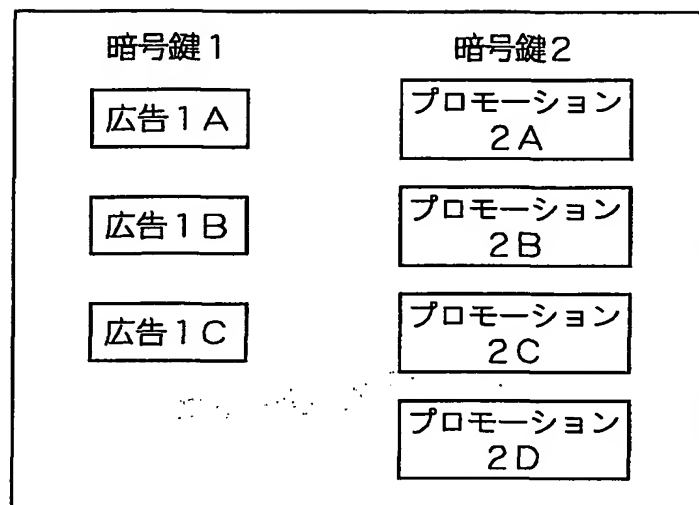


Fig. 26

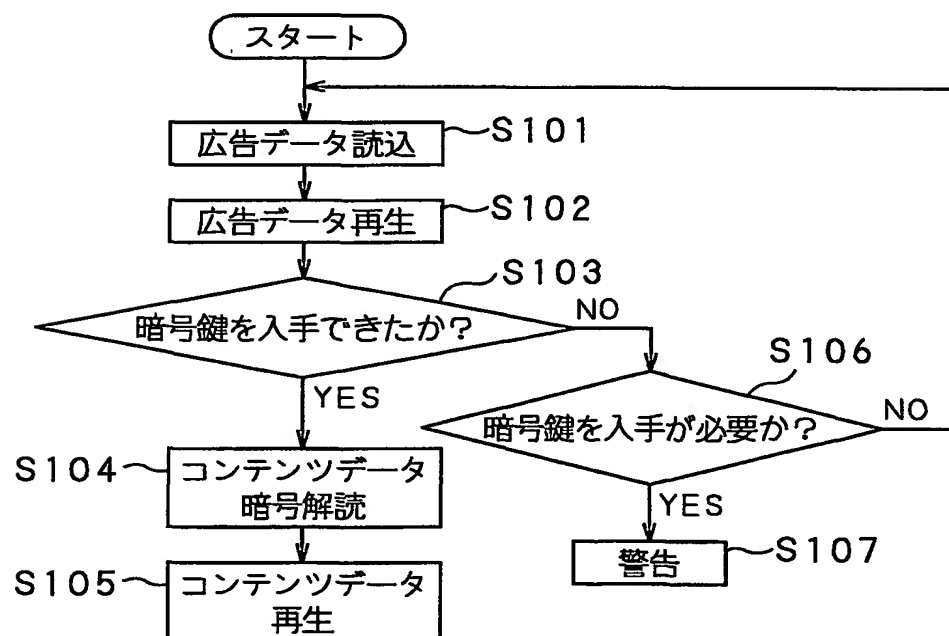


Fig. 27

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/06663

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L9/00, G06F17/60, H04N5/92, G11B20/10, G11B20/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L9/00, G06F17/60, H04N5/92, G11B20/10, G11B20/12

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
 Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, INSPEC, JICST Database on Science and Technology, advertisement,
 ad., encryption, key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 10-164550 A (Toshiba Corporation), 19 June, 1998 (19.06.98), Claim 1; Par. Nos. [0033] to [0060], [0125] to [0130] (Family: none)	1, 2, 5-12, 14-35, 37-51
Y		52-56
A		3, 4, 13, 36
Y	JP 11-196084 A (Matsushita Electric Ind. Co., Ltd.), 21 July, 1999 (21.07.99), Par. Nos. [0031] to [0036] (Family: none)	52-56
A		3, 4, 13, 36

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:
 "A" document defining the general state of the art which is not
 considered to be of particular relevance
 "E" earlier document but published on or after the international filing
 date
 "L" document which may throw doubts on priority claim(s) or which is
 cited to establish the publication date of another citation or other
 special reason (as specified)
 "O" document referring to an oral disclosure, use, exhibition or other
 means
 "P" document published prior to the international filing date but later
 than the priority date claimed

"T" later document published after the international filing date or
 priority date and not in conflict with the application but cited to
 understand the principle or theory underlying the invention
 "X" document of particular relevance; the claimed invention cannot be
 considered novel or cannot be considered to involve an inventive
 step when the document is taken alone
 "Y" document of particular relevance; the claimed invention cannot be
 considered to involve an inventive step when the document is
 combined with one or more other such documents, such
 combination being obvious to a person skilled in the art
 "&" document member of the same patent family

Date of the actual completion of the international search
 29 October, 2001 (29.10.01)

Date of mailing of the international search report
 06 November, 2001 (06.11.01)

Name and mailing address of the ISA/
 Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

THIS PAGE BLANK (USPTO)

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/00, G06F17/60, H04N5/92, G11B20/10,
G11B20/12

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/00, G06F17/60, H04N5/92, G11B20/10,
G11B20/12

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2001年
 日本国登録実用新案公報 1994-2001年
 日本国実用新案登録公報 1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

WPI, INSPEC, JICST 科学技術文献データベース advertisement, ad., encryption, key

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 10-164550 A (株式会社東芝) 19. 6月. 1998 (19. 06. 98), 請求項1, 第33-60, 125-130段落 (ファミリーなし)	1, 2, 5-12, 14 -35, 37-51
Y		52-56
A		3, 4, 13, 36
Y	JP 11-196084 A (松下電器産業株式会社) 21. 7月. 1999 (21. 07. 99), 第31-36段落 (ファミリーなし)	52-56
A		3, 4, 13, 36

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

29. 10. 01

国際調査報告の発送日

06.11.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
 郵便番号100-8915
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中里 裕正

5M

9364

電話番号 03-3581-1101 内線 3597

THIS PAGE BLANK (USPTO)